

COMPLIANCE  
OF CYBER  
SECURITY LAW

# 网络安全 法律遵从

马民虎◎主编

360法律研究院◎组织编写

电子工业出版社  
Publishing House of Electronics Industry  
北京·BEIJING

## 内 容 简 介

本书针对企业网络安全法律遵从的实际需求,以《中华人民共和国网络安全法》(以下简称《网络安全法》)为分析蓝本,从相关法条释义和解读、网络安全相关制度概述、典型案例解析等方面,梳理和分析了一般网络运营者、关键信息基础设施运营者,以及网络产品和服务提供者的网络安全法律遵从框架与实施建议,以期为相关企业遵从《网络安全法》及其制度要求提供可操作性指引。本书分为四个部分,分别是《网络安全法》导论、一般网络运营者的网络安全法律遵从、关键信息基础设施运营者的网络安全法律遵从及网络产品和服务提供者的网络安全法律遵从。

未经许可,不得以任何方式复制或抄袭本书之部分或全部内容。  
版权所有,侵权必究。

## 图书在版编目(CIP)数据

网络安全法律遵从/马民虎主编. —北京:电子工业出版社,2018.2  
ISBN 978-7-121-33249-4

I. ①网… II. ①马… III. ①计算机网络—科学技术管理法规—中国 IV. ①D922.17  
中国版本图书馆 CIP 数据核字(2017)第 306228 号

策划编辑:戴晨辰

责任编辑:戴晨辰 文字编辑:韩玉宏

印 刷:

装 订:

出版发行:电子工业出版社

北京市海淀区万寿路 173 信箱 邮编 100036

开 本:720×1 000 1/16 印张:28.75 字数:499 千字

版 次:2018 年 2 月第 1 版

印 次:2018 年 2 月第 1 次印刷

定 价:79.00 元

凡所购买电子工业出版社图书有缺损问题,请向购买书店调换。若书店售缺,请与本社发行部联系,联系及邮购电话:(010) 88254888, 88258888。

质量投诉请发邮件至 [zltts@phei.com.cn](mailto:zltts@phei.com.cn), 盗版侵权举报请发邮件至 [dbqq@phei.com.cn](mailto:dbqq@phei.com.cn)。

本书咨询联系方式: [dcc@phei.com.cn](mailto:dcc@phei.com.cn)。

# 编委会

Editorial Committee

(按姓氏笔画排序)

马民虎 马 宁 王 玥 方 婷  
许 坚 江智茹 张 敏 张素伦  
李海英 赵丽莉 赵 军 唐治国  
黄道丽 傅 敏





# 前言

## Preface

网络安全事关国家利益，而网络空间中的国家利益冲突极其尖锐，其中军事冲突、进出口管控，以及国家安全审查、数据主权等方面的国际斗争日趋激烈。在互联网迅速发展的时代，网络安全已成为影响国家安全和稳定的关键问题，成为国家安全体系的重要组成部分。网络安全和信息化对一个国家的很多领域来说都是牵一发而动全身的，没有网络安全就没有国家安全。鉴于网络安全在国家安全中的重要性，以及网络安全面临的复杂形势，制定网络安全法，提高网络治理的法治化水平已是必然。

2016年11月7日，第十二届全国人民代表大会常务委员会（以下简称“全国人大常委会”）第二十四次会议通过《中华人民共和国网络安全法》（以下简称《网络安全法》），并于2017年6月1日起正式实施，共7章，79条。《网络安全法》是我国信息安全领域的重大立法，它体现了国家对建立健全网络空间秩序的基本意志。该法确立了“保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织合法权益，促进经济社会信息化健康发展”的立法目标，调整范围包括中华人民共和国境内建设、运营、维护和使用的网络，以及网络安全的监督管理，具体内容涉及网络安全支持与促进、网络运行安全、网络信息安全、监测预警与应急处置、法律责任等方面。《网络安全法》的制定和实施响应了习近平总书记提出的“全天候全方位感知网络安全态势”的基本要求，是依法治网的一个重大立法举措，弥补了网络安全法律保障机制上位法

律制度的缺失，对配套法律法规的制定和具体制度的实施具有重要的指导作用。

本书以《网络安全法》为分析蓝本，以企业网络安全法律遵从为视角，围绕《网络安全法》相关法条释义和解读、网络安全相关制度概述、典型案例解析等方面，梳理和分析了一般网络运营者、关键信息基础设施运营者，以及网络产品和服务提供者这三类遵从主体的网络安全法律遵从框架和实施建议，以期为企业遵从《网络安全法》及其制度要求提供可操作性指引。本书框架由方婷、郑蕾、赵军、张素伦共同讨论，章节框架最后由马民虎、许坚确定，方婷、郑蕾统筹实施，书稿分为以下四个部分。

第一部分（第1章~第4章）为《网络安全法》导论。该部分重点梳理和分析了国内外网络安全态势、国内外网络安全事件与立法，以及《网络安全法》的基本原理。马民虎、方婷、梁思雨、张若琳、马可、张敏、党家玉负责本部分的撰写工作。

第二部分（第5章~第12章）重点分析了一般网络运营者的网络安全法律遵从。该部分分别从网络安全等级保护制度，网络实名制，网络安全监测预警和应急响应，安全认证、检测及风险评估，网络安全信息披露，协助执法，个人信息保护，以及网络信息内容过滤等方面分析已有网络安全法律制度对一般网络运营者提出的法律遵从要求。黄道丽、王玥、赵丽莉、李海英、方婷、赵光、何治乐、唐治国、马可、冯潇洒、党家玉、梁思雨负责本部分的撰写工作。

第三部分（第13章~第17章）重点分析了关键信息基础设施运营者的网络安全法律遵从。该部分首先对关键信息基础设施的界定及其范围进行解读，并进一步针对关键信息基础设施运营者的安全保护义务、网络安全审查要求、数据本地化与跨境传输要求、网络安全信息共享要求等提出我国关键信息基础设施运营者的网络安全法律遵从框架及建议。赵婧琳、张敏、马宁、郑蕾、梁思雨、方婷和马悦负责本部分的撰写工作。

第四部分（第18章~第22章）重点分析了网络产品和服务提供者的网络安全法律遵从。该部分在对《网络安全法》关于网络产品和服务提供者规定的基础上，围绕网络产品和服务安全、网络安全漏洞通知和报告、用户信息保护、保密义务、网络关键设备和网络安全专用产品强制认证等方面重点分析了网络产品和服务提供者的网络安全法律遵从框架及建议。黄道丽、方婷、江智茹、党家玉、张若琳、梁志伟负责本部分的撰写工作。

# 目录

## Contents

### 第一部分 《网络安全法》导论

第 1 章 国内外网络安全态势 .....	3
态势一：各国普遍将网络安全提升到国家战略层面 .....	4
态势二：关键信息基础设施安全隐患增多，搭建网络空间基础防御 .....	7
态势三：网络谣言、网络恐怖主义肆虐，网络内容治理迫在眉睫 .....	10
态势四：勒索软件等网络攻击事件频发，数据泄露问题严重 .....	12
态势五：重视国际网络空间治理，构建网络空间命运共同体 .....	13
第 2 章 国外网络安全立法与事件 .....	15
第一节 网络安全规制形式 .....	15
第二节 国外主要国家及地区网络安全立法情况概述 .....	16
第三节 国外网络安全事件概要 .....	28
第 3 章 我国网络安全立法与事件 .....	32
第一节 1999 年以前 .....	32
第二节 1999—2005 年 .....	33
第三节 2005—2012 年 .....	36
第四节 2012 年至今 .....	40

第4章 《网络安全法》的基本原理 .....	45
第一节 《网络安全法》的制定背景 .....	45
第二节 《网络安全法》与相关立法的关系 .....	49
第三节 《网络安全法》的基本原则 .....	57
第四节 《网络安全法》的调整对象 .....	61
第五节 《网络安全法》的行为准则 .....	65

## 第二部分 一般网络运营者的网络安全法律遵从

第5章 网络安全等级保护制度 .....	73
第一节 《网络安全法》相关规定及释义 .....	73
第二节 网络安全等级保护制度概述 .....	80
第三节 网络安全等级保护法规遵从框架及建议 .....	86
第四节 监督管理与法律责任 .....	95
第6章 实名制与可信身份战略 .....	98
第一节 《网络安全法》相关规定及释义 .....	98
第二节 网络实名制与可信身份战略制度概述 .....	99
第三节 网络实名制的法规遵从框架及建议 .....	101
第四节 监督管理与法律责任 .....	104
第7章 网络安全监测预警和应急响应 .....	105
第一节 网络安全监测与信息收集 .....	106
第二节 网络安全信息分析与预警研判 .....	115
第三节 网络安全信息通报 .....	120
第四节 网络安全预警信息发布 .....	129
第五节 网络安全事件应急预案 .....	135
第六节 网络安全事件应急响应机制 .....	153
第七节 网络安全事件应急演练 .....	165
第八节 网络安全监督管理约谈措施 .....	174

第九节 网络通信临时管制	180
第十节 突发事件应对	184
<b>第 8 章 安全认证、检测及风险评估</b>	<b>193</b>
第一节 《网络安全法》相关规定及释义	193
第二节 网络安全认证、检测及风险评估制度概述	205
第三节 网络安全认证、检测及风险评估法规遵从框架及建议	206
<b>第 9 章 网络安全信息披露</b>	<b>221</b>
第一节 《网络安全法》相关规定及释义	221
第二节 网络安全信息披露制度概述	222
第三节 网络安全信息披露法规遵从框架及建议	226
第四节 典型案例	229
第五节 监督管理与责任	233
<b>第 10 章 协助执法</b>	<b>234</b>
第一节 《网络安全法》相关规定及释义	234
第二节 协助执法制度概述	236
第三节 典型案例	246
第四节 协助执法制度的法规遵从框架及建议	251
<b>第 11 章 个人信息保护</b>	<b>255</b>
第一节 《网络安全法》相关规定及释义	255
第二节 个人信息保护制度概述	258
第三节 典型案例	263
第四节 个人信息保护的法规遵从框架及建议	266
第五节 监督管理与法律责任	280
<b>第 12 章 网络信息内容过滤</b>	<b>282</b>
第一节 《网络安全法》相关规定及释义	283

第二节 网络信息内容过滤制度概述·····	285
第三节 网络信息内容过滤法规遵从框架及建议·····	288
第四节 监督管理与法律责任·····	290

### 第三部分 关键信息基础设施运营者的网络安全法律遵从

第 13 章 关键信息基础设施的界定及其范围·····	297
第一节 国外关键信息基础设施概念的界定及其范围·····	297
第二节 我国关键信息基础设施概念的提出及范围界定·····	304
第三节 我国关键信息基础设施的界定主体·····	308
第 14 章 安全保护义务·····	309
第一节 《网络安全法》相关规定及释义·····	310
第二节 关键信息基础设施运营者安全保护义务制度概述·····	311
第三节 关键信息基础设施运营者安全保护义务法规遵从框架及建议·····	316
第四节 监督管理与法律责任·····	321
第 15 章 网络安全审查·····	323
第一节 《网络安全法》相关规定及释义·····	323
第二节 网络安全审查制度概述·····	325
第三节 美英网络安全审查的相关实践·····	331
第四节 我国网络安全审查制度法规遵从框架及建议·····	340
第 16 章 数据本地化与跨境传输·····	346
第一节 《网络安全法》相关规定及释义·····	346
第二节 数据本地化·····	347
第三节 数据跨境传输安全评估·····	354
第四节 监督管理与法律责任·····	363
第 17 章 网络安全信息共享·····	365
第一节 《网络安全法》相关规定及释义·····	366

第二节 网络安全信息共享制度概述·····	372
第三节 网络安全信息共享法规遵从框架及建议·····	382
第四节 监督管理与法律责任·····	389
 <b>第四部分 网络产品和服务提供者的网络安全法律遵从</b>	
<b>第 18 章 网络产品和服务安全·····</b>	<b>393</b>
第一节 《网络安全法》相关规定及释义·····	393
第二节 网络产品和服务安全保障制度概述·····	394
第三节 网络产品和服务安全保障法规遵从框架及建议·····	396
第四节 监督管理与法律责任·····	398
 <b>第 19 章 网络安全漏洞通知和报告·····</b>	 <b>400</b>
第一节 《网络安全法》相关规定及释义·····	400
第二节 网络安全漏洞通知和报告制度概述·····	401
第三节 网络安全漏洞通知和报告法规遵从框架及建议·····	405
第四节 监督管理与法律责任·····	409
 <b>第 20 章 用户信息保护·····</b>	 <b>411</b>
第一节 《网络安全法》相关规定及释义·····	411
第二节 网络产品和服务的用户信息保护制度概述·····	412
第三节 网络产品和服务的用户信息保护法规遵从框架及建议·····	426
第四节 监督管理与法律责任·····	433
 <b>第 21 章 保密义务·····</b>	 <b>434</b>
第一节 《网络安全法》相关规定及释义·····	434
第二节 保密义务制度概述·····	435
第三节 保密义务法规遵从框架及建议·····	438
第四节 监督管理与法律责任·····	441

第 22 章 网络关键设备和网络安全专用产品合规要求 .....442

    第一节 《网络安全法》相关规定及释义 .....442

    第二节 网络关键设备和网络安全专用产品合规制度概述 .....443

    第三节 网络关键设备和网络安全专用产品合规法规遵从框架及建议 .....444

    第四节 监督管理与法律责任 .....446



# Part 1

## 第一部分

### 《网络安全法》导论

第 1 章 国内外网络安全态势

第 2 章 国外网络安全立法与事件

第 3 章 我国网络安全立法与事件

第 4 章 《网络安全法》的基本原理



# 国内外网络安全态势

人类社会的发展至今，先后经历了农业革命和工业革命，当前正在历经信息革命。信息革命作为经济全球化的重要推动力量，引领了社会生产新变革，创造了人类生活新空间，拓展了国家治理新领域，极大地提高了人类认识世界、改造世界的能力。随着全球信息化的发展和深入推进，网络与经济社会各领域深层次融合，网络在极大地促进经济社会繁荣进步的同时，其带来的安全威胁和风险也日益突出，特别是针对关键信息基础设施的重大网络安全事件，例如，针对乌克兰电网发起的攻击造成基础电力运行的崩溃；针对伊朗核设施的攻击使其被迫暂停核运行；针对美国 Dyn 域名服务提供商进行的分布式拒绝服务（Distributed Denial of Service, DDoS）攻击使大量网站陷入瘫痪，造成的灾难性后果已严重危害国家经济安全和公共利益。与此同时，网络恐怖主义、网络诈骗、网络谣言等的恶意蔓延也直接威胁人们的生命财产安全，影响社会和谐稳定，长此以往将导致人们对网络安全的不信任，抑制信息化的发展。因此，网络安全已经成为事关人类共同利益，事关世界和平与发展，事关国家安全的重要一环。

近年来，新一代信息技术蓬勃发展，大数据、云计算、物联网等在带来便利的同时，也引发了新的网络安全问题。云计算需要汇集海量的数据从而进行整合处理，使得数据的跨境流动成为常态，数据主体对于数据资源的控制力持续削弱。“棱镜门”事件的爆发使得各国开始意识到此种削弱使得数据本身的安

全性和由数据所承载的国家安全、社会稳定和个人信息都面临潜在威胁，数据的主权界定也就成为亟待解决的问题。与此同时，各国政府和私有部门纷纷在物联网和人工智能等新兴信息技术领域投入更多资源，使其逐渐成为恶意网络分子利用的工具，网络攻击手段更加复杂，溯源难度进一步增加，而物联网和人工智能技术本身引起的隐私保护和道德伦理等问题也摆在眼前。因此，无论是出于保护传统网络安全，还是维护新兴技术发展的目的，各国都充分认识到网络安全对于国家、社会和公民的价值，普遍将其提升到国家战略层面，并且针对关键信息基础设施、网络恐怖主义、网络谣言及数据保护等内容完善立法，同时，加强国际合作，提升网络空间的国际话语权，构建网络空间国际治理规则。

## 态势一：各国普遍将网络安全提升到国家战略层面

网络空间已经成为与海、陆、空和外层空间同等重要的人类活动新领域。在国际社会，对于网络这一第五空间的关注从未停止，国家政治、经济、文化、国防及公民在网络空间的合法权益皆面临严峻挑战。近年来，各国在推动网络核心技术、新兴技术发展的基础上，将安全理念从局部安全拓展为全面安全，将中长期发展战略、网络安全人才培养、国际合作等内容也囊括在内。我国于 2014 年提出总体国家安全观，将国家安全置于国家治理的大背景下来思考和筹划，将安全治理作为基本路径来维护和保障。坚持总体国家安全观，体现在治理实践上，就是推进国家安全总体治理；既重视传统安全，又重视非传统安全，构建集政治安全、国土安全、军事安全、经济安全、文化安全、社会安全、科技安全、信息安全、生态安全、资源安全、核安全等于一体的国家安全体系；走出一条中国特色国家安全道路，在安全各领域、各要素、各层面统筹治理，创建当代中国国家安全治理系统格局。

国际社会，2011 年，美国出台《网络空间国际战略》（International Strategy for Cyberspace）宣称要建立一个“开放、互通、安全和可靠”的网络空间，并为

实现这一构想勾勒出了政策路线图，内容涵盖经济、国防、执法和外交等领域。

近几年美国又先后公布《网络空间政策审查》(Cyberspace Policy Review)、《国际网络战略网络世界的繁荣、安全和开放》(International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World)、《改善关键基础设施网络安全的行政令》(Improving Critical Infrastructure Cybersecurity)、《2014 年网络安全增强法案》(Cybersecurity Enhancement Act of 2014)、《2014 年国家网络安全保护法》(National Cybersecurity Protection Act of 2014)、《改进关键基础设施网络安全草案》(Draft Strategy for Improving Critical Infrastructure Cybersecurity)、《国家安全战略》(National Security Strategy)、《国防部网络战略》(The Department of Defence Cyber Strategy)、《2015 年网络安全法案》(Cybersecurity Act of 2015)、《增强联邦政府网络与关键基础设施网络安全的行政令》(Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure)等一系列法律规范和政策，着眼于在提升网络安全应急和防御能力的同时建立本国的网络部队，同步培育自卫能力和对外威慑力。

与此同时，欧盟也颁布《欧盟网络安全战略：公开、可靠和安全的网络空间》(Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace)、《欧盟网络防御政策框架》(EU Cyber Defence Policy Framework)、《欧洲安全议程》(The European Agenda on Security)、《欧洲议会和欧盟理事会关于自然人个人数据处理和数据自由流动保护，并废除 95/46/EC 号指令的第 2016/680 号条例（通用数据保护条例）》<sup>①</sup>、《欧盟网络与信息系统安全指令》(The Directive on Security of Network and Information Systems)、《欧洲议会和欧盟理事会关于欧盟高级别网络和信息系统安全措施的第 2016/1148 号指令》<sup>②</sup>等，强调成员国间、成员内部政府、企业和社会服务等机构之间的信息共享与交流合作，致力于共同维护网络安全。

逐渐脱欧的英国为保障本国在数据时代的安全和繁荣，先后公布《动荡时代

---

① Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) .

② Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

强大的英国：国家安全战略》(A Strong Britain in an Age of Uncertainty: The National Security Strategy)、《紧急通信与互联网数据保留法案》(Data Retention and Investigatory Powers Act)、《2016—2021 年国家网络安全战略》(National Cyber Security Strategy 2016—2021) 等，重视培养网络安全人才，赋予英国政府更多执法权力。

作为我国邻国的俄罗斯也不甘示弱，先后公布《关于俄罗斯联邦武装力量在信息空间活动的概念性观点》(Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space)、《俄罗斯联邦国际信息安全领域国家政策基本原则》(Basic Principles for State Policy of the Russian Federation in the Field of International Information Security)、《俄罗斯联邦外交政策理念》(Concept of the Foreign Policy of the Russian Federation)、《俄罗斯联邦军事理论》(Military Doctrine of the Russian Federation)、《俄罗斯网络安全战略概念—进行中的草案》(Concept of Russia's Cyber Security Strategy - Draft Underway)、《俄罗斯联邦国家安全战略》(National Security Strategy of the Russian Federation)、《续展进行中—俄罗斯联邦信息安全理论》(Renewal Underway-Information Security Doctrine of the Russian Federation)，保障网络安全。

我国接入国际互联网只有 20 多年，起步较晚。但当前面临的网络安全形势同样异常复杂，安全任务同样艰巨。对此，我国政府层面对网络安全领域给予高度重视，先后公布《国家网络空间安全战略》、《信息产业发展指南》、《信息通信行业发展规划（2016—2020 年）》、《大数据产业发展规划（2016—2020 年）》、《软件和信息技术服务业发展规划（2016—2020 年）》、《网络空间国际合作战略》、《云计算发展三年行动计划（2017—2019 年）》等，就我国网络安全国内外发展形势加以概括性指导。其中《国家网络空间安全战略》站在宏观角度，对我国网络安全治理提出四点基本原则，即尊重维护网络空间主权、和平利用网络空间、依法治理网络空间、统筹网络安全与发展，并将坚定捍卫网络空间主权、坚决维护国家安全、保护关键信息基础设施、加强网络文化建设、打击网络恐怖和违法犯罪、完善网络治理体系、夯实网络安全基础、提升网络空间防护能力和强化网络空间国际合作作为今后发展的九大战略任务，为我国今后的网络治理指明了方向。

而《网络空间国际合作战略》是我国就网络问题首次发布国际战略，体现了

我国就网络空间积极拓展国际合作、构建网络空间命运共同体的信心和决心。该战略以和平发展为主题；以合作共赢为核心；倡导“和平、主权、共治、普惠”作为网络空间国际交流与合作的基本原则，以维护主权和安全、构建国际规则体系、促进互联网公平治理、保护公民合法权益、促进数字经济合作、打造网上文化交流平台为战略目标；从倡导和维护网络空间和平与稳定、推动构建以规则为基础的网络空间秩序、不断拓展网络空间伙伴关系、积极推进全球互联网治理体系改革、深化打击网络恐怖主义和网络犯罪、倡导对隐私权等公民权益保护、推动数字经济发展和数字红利普惠共享、加强全球信息基础设施建设和保护、促进网络文化交流互鉴这九个方面提出了中国推动并参与网络空间国际合作的行动计划；明确我国始终是网络空间的建设者、维护者和贡献者，彰显了我国作为互联网大国的责任与风范。

而网络空间的竞争，归根结底是人才的竞争。总体而言，我国网络安全人才还存在数量缺口较大、能力素质不高、结构不合理等问题，与维护国家网络安全、建设网络强国的要求不相适应。为此，就网络安全人才培养方面，我国公布了《关于加强网络安全学科建设和人才培养的意见》，旨在为我国网络安全事业提供充足的人才储备，并且重视新生代网络安全人才能力与使命感的培养。

在此过程中，网络运营者不仅作为一个法律法规遵从主体，将国家战略、法律法规要求落到实处，使之从真正意义上实现应有的秩序价值和引导价值。同时，网络运营者处在市场第一线，对于技术缺口和现实需求的感知更加及时和准确，在网络空间治理层面可充分发挥自身优势，为国家完善法律制度体系，更好地进行网络社会治理建言献策，构建良好的市场环境和国际氛围。

## 态势二：关键信息基础设施安全隐患增多， 搭建网络空间基础防御

随着网络与信息技术的飞速发展，传统的物理基础设施与信息系统的融合程度不断加深，在国家安全、社会稳定、经济发展方面的基础性作用日益凸显，对于其稳定性和安全性的妥善保障意义重大。《国家网络空间安全战略》中将关键信

息基础设施定义为关系国家安全、国计民生，一旦数据泄露、遭到破坏或者丧失功能可能严重危害国家安全、公共利益的信息设施，包括但不限于提供公共通信、广播电视传输等服务的基础信息网络，能源、金融、交通、教育、科研、水利、工业制造、医疗卫生、社会保障、公用事业等领域和国家机关的重要信息系统，重要互联网应用系统等。从此概念界定可以看出，关键信息基础设施安全关乎社会基本运行，是经济社会运行的神经中枢，是网络安全的重中之重，也是可能遭到重点攻击的目标。关键信息基础设施一旦遭受网络攻击就可能造成交通中断、金融紊乱、电力瘫痪等问题，具有很大的破坏性和杀伤力。

“震网”病毒、“Duqu”病毒和“火焰”病毒等攻击事件的出现，充分印证了网络威胁正在向工业控制系统、能源、交通、金融、电力等关键领域快速蔓延。如果不加以妥善治理，不仅严重影响到国家关键信息基础设施的持续正常运行，还将使国家和社会稳定面临前所未有的威胁。2016 年 10 月美国发生大规模网络瘫痪事件，包括 twitter、spotify、netflix、airbnb、github、reddit 及《纽约时报》等主要网站都受到影响，一时间网络无法访问对社会基本运营造成恶劣影响。经调查此次事件发生的原因在于美国网络服务供应商迪恩公司的服务器遭到了分布式拒绝服务攻击。迪恩公司作为美国主要域名服务器（Domain Name System, DNS）供应商，其客户包括多家业内巨头和知名互联网公司。而 DNS 是互联网运作的核心，主要职责就是将用户输入的内容翻译成计算机可以理解的 IP 地址，从而将用户引入正确的网站。一旦遭到攻击，用户就无法登录网站。除了传统信息技术面临威胁外，近年来快速发展的移动互联网、物联网、云计算、大数据、人工智能等新一代信息技术，也将产生无法预知的风险。

作为网络社会的基础设施，世界各国对其保障都给予了足够的重视。1998 年，美国发布《第 63 号总统令》（PDD 63），制订和实施保护政府的基础设施计划，同时鼓励政府与私有部门之间展开对话，开始构建关键信息基础设施保护体系。自此之后，美国发布 2000 年《信息系统保护国家计划》（National Plan for Information Systems Protection）、2001 年《爱国者法案》（Patriot Act）、2002 年《关键基础设施信息保护法》（Critical Infrastructure Information Act of 2002）、2003 年《关键基础设施和重要资产物理保护国家战略》（The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets）、2003 年《保护网络空间



国家战略》(The National Strategy to Secure Cyberspace)、2003 年《国土安全总统第 7 号 令》(Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection)、2013 年《提高关键基础设施的安全性和恢复力》(PPD 21)等法案,明确关键信息基础设施范围、保护方式及共享手段。

与此同时,欧盟出台 2005 年《保护关键基础设施的欧洲计划》、2006 年《关于欧盟理事会制定识别、指定欧洲关键基础设施,并评估提高保护必要性的指令建议》(Proposal for a directive of the council on the identification and designation of European critical infrastructure and the assessment of the need to improve their protection 2006)、2012 年《欧洲议会关于关键信息基础设施保护的成就与展望:面向全球网络安全的决议》[Critical information infrastructure protection: towards global cyber-security European Parliament resolution of 12 June 2012 on critical information infrastructure protection – achievements and next steps: towards global cyber-security (2011/2284 (INI))]等内容,确立关键信息基础设施认定标准,强化职能分工与协作。

我国对于关键信息基础设施保护也给予充分重视,《国家网络空间安全战略》将保护关键信息基础设施作为战略任务之一,强调关键信息基础设施保护是政府、企业和全社会的共同责任,要采取一切必要措施保护关键信息基础设施及其重要数据不受攻击破坏。《网络空间国际合作战略》同样将加强全球信息基础设施建设和保护作为行动计划之一,明确要加强关键信息基础设施及其重要数据的安全防护,推动各国就关键信息基础设施保护达成共识,制定关键信息基础设施保护的合作措施,加强关键信息基础设施保护的立法、经验和技术交流,推动加强各国在预警防范、应急响应、技术创新、标准规范、信息共享等方面合作,提高网络风险的防范和应对能力。《网络安全法》中设立专门章节规定关键信息基础设施的保护,此外,作为落实的配套制度,2017 年 7 月 10 日,国家互联网信息办公室就《关键信息基础设施安全保护条例(征求意见稿)》向社会公开征求意见,保障关键信息基础设施安全。

在此过程中,网络运营者,特别是涉及关键信息基础设施的运营者对于此类安全保障可发挥难以替代的价值。在运营过程中,将国家网络安全要求落到实处,提高自身网络安全意识,以高标准、严要求处理日常隐患。在攻击事件发生前,

有条件的网络运营者及时发现和接收监测预警信息，并通过上通下达或共享平台将信息加以扩散，减少不必要的损失。在事件发生过程中，有效启动相应等级的应急响应预案，向社会公布安全事件信息和应对措施，安抚社会情绪。在近期发生的“WannaCry”勒索病毒事件中，微软及我国的安天等网络运营者第一时间公布了相应的官方公告或防护手册，引导用户进行处理。同时在事件发生过程中注意留存相关攻击数据，为后续溯源和追责提供依据。在事件发生后，及时向行业主管或监管部门报告，检查系统漏洞并加以修复，提升系统和设备安全性，从而形成良性的关键信息基础设施保护体系。

### 态势三：网络谣言、网络恐怖主义肆虐， 网络内容治理迫在眉睫

在移动互联网和各类社交媒体快速发展的环境下，人们的日常沟通交流已经突破物理地域或距离上的限制，即时通信工具的普及极大地加速了信息的传播速度，这在便利生产生活的同时，也间接助长了网络谣言、虚假信息的扩散。现如今，网络谣言、虚假信息泛滥引发信息内容失控，已成为一种公害，不仅严重侵害了公民切身利益，也严重扰乱了网络公共秩序，直接危害社会稳定。同时，利用网络宣传思想、招募人才也成为恐怖组织的惯用伎俩，宣扬恐怖主义、极端主义，散播暴恐音视频，煽动颠覆国家政权等行为借助网络的传播与扩散，严重危害国家安全和社会公共利益。

在 2017 年“WannaCry”勒索病毒刚刚爆发时，我国部分媒体一度宣扬教育网是勒索软件的重灾区，报道称“大量准毕业生的毕业设计、论文材料被加密，导致无法完成论文答辩”、“整个教育行业损失非常严重”等内容，一时间使得社会对教育网安全性产生担忧，影响高校学生对于网络的使用。而中国教育和科研计算机网于 5 月 15 日发表声明，斥责关于教育网“大面积感染勒索病毒”的不实报道，指出经统计，教育网并未出现大规模勒索病毒感染，也不是重灾区<sup>①</sup>。据微

<sup>①</sup> 参考 [http://www.edu.cn/info/focus/rd\\_xin\\_wen/201705/t20170515\\_1516270.shtml](http://www.edu.cn/info/focus/rd_xin_wen/201705/t20170515_1516270.shtml)。

信安全中心公布的 2016 年度十大谣言显示，谣言多涉及儿童守护站类、“SB250 病毒”系列谣言、收文件有毒类、偷卖儿童类、儿童用药类等谣言，内容与人们日常生活息息相关。“7·23 动车事件”中外籍旅客政府天价赔偿事件、日本核危机引发的大量囤盐事件更是导致了社会舆论的歪曲和运行的混乱。在移动互联网普及的时代，不实言论或虚假消息的传播速度又十分迅速，如果国家权威机构无法及时澄清，对消息和言论的发布者、传播者不能依法追责，重则危机社会稳定和良好运行，轻则影响人们的正常生产生活。

网络恐怖主义是影响国际和平与安全的新威胁。极端组织“伊斯兰国”（IS）经常使用社交网站、手机应用等互联网手段宣传极端思想，招募成员。在推特等社交媒体和网络论坛中散发煽动性的文字、图片、视频，引诱人们观看和传播，加速了网络恐怖主义的蔓延趋势。目前我国已出现大量利用网络传播暴恐音视频的现实案例，犯罪分子通常出于盈利或为寻求刺激、吸引点击量的目的，利用 QQ、微信等即时通信工具下载、传播暴恐音视频，这容易对心智尚不完全成熟的未成年人造成误导。需要国家采取切实措施，打击网络恐怖主义活动，防范恐怖分子利用网络宣传恐怖极端思想，策划和实施恐怖主义活动。

在治理层面，各国多采用政府主导、行业自律与公民参与的综合治理模式：通过国家及时监测、识别、澄清网络谣言，整治网络恐怖主义内容，行业加强自我约束和内部管理，公民广泛参与，对危害内容积极举报等手段实现网络信息内容治理。在我国，通过《中华人民共和国刑法》（以下简称《刑法》）、《治安管理处罚法》、《互联网信息服务管理办法》、《反恐怖主义法》、《网络安全法》等强化事前警示、事中监管和事后追惩。并且，通过开通中国互联网违法和不良信息举报中心、中国食品辟谣网等官方网站及时接受公民举报和澄清谣言信息。

对于网络运营者而言，其直接面向网络谣言和恐怖主义等不良信息肆虐的平台或媒介，因此应充分承担其应有的法律义务和社会责任，充分发挥自身信息挖掘和收集优势，识别自身运营平台中潜在的恐怖主义及敏感信息，收集网络谣言等不良信息并在一定条件下向社会加以公布。Facebook 近期采取了一系列措施治理和打击谣言传播，我国部分互联网企业也通过自身平台或渠道及时公布相关内容，与政府共建清朗文明的网络空间。

## 态势四：勒索软件等网络攻击事件频发， 数据泄露问题严重

数据是互联网时代最有价值的资源，加强包括个人信息在内的数据安全保护不论是对国家，还是对企业和个人而言都有现实意义。然而，正因为数据的价值巨大，近年来规模不一的数据泄露事件屡屡发生。根据数字安全研究公司金雅拓公司（Gemalto）最新发布的报告显示，2016 年共发生 1 800 起数据泄露事件，导致近 14 亿条记录外泄，相比 2015 年增加了 86%<sup>①</sup>。在近期发生的数据泄露事件中，波及范围从国家关键领域，如美国国防部、日本政府网站等各国政务系统、大型移动服务提供商等，到大规模公民个人信息泄露，诸如雅虎 10 亿个邮箱账户信息泄露事件、“58 同城”简历信息泄露事件等。数据泄露事件的发生一方面导致个人对于企业、社会乃至国家网络安全保护水平的不信任，从而一定程度上抑制了网络的发展，另一方面，大量重要数据、个人信息的泄露对于国家安全、社会稳定和个人利益都将造成潜在威胁。电信诈骗的层出不穷，“徐玉玉”等一系列案件的发生敲响了数据安全保护的警钟。

在当前治理模式下，对于数据保护呈现两个特点。第一，不断加强个人信息保护，赋予信息主体更多的知情权和选择权。被遗忘权的提出、企业收集数据必须获得用户明示同意等制度的出现，更加全面地保护了信息安全。第二，重视跨境数据的安全保护。在经济全球化和大型互联网企业快速发展的背景下，加上云计算、大数据等新一代信息技术的助推，使得数据的跨境流动成为常态。不论是企业内部的数据流转还是单纯的数据贸易，跨境的过程使得数据主体对于数据的控制力持续削弱，并且当前“棱镜门”事件引发的外国监听威胁仍存在，数据的跨境流动将在一定程度上增加数据面临的潜在威胁。在欧盟 2018 年即将生效的《通用数据保护条例》中专门规定了数据跨境流动前的安全评估政策，需保证数据接收国或地区保持与本国同等的数据保护水平。在现存国际组织、正在进行的区

<sup>①</sup> 参考 <http://breachlevelindex.com/assets/Breach-Level-Index-Report-2016-Gemalto.pdf>。

域性国家合作组织谈判过程中都或多或少地涉及跨境数据的安全问题。

在我国当前的数据保护立法体系中，对于上述特点也都有所体现。《信息安全技术个人信息保护指南》、《全国人大常委会关于加强网络信息保护的決定》、《信息安全技术公共及商用服务信息系统个人信息保护指南》、《电信和互联网用户个人信息保护规定》、《网络安全法》第四章等对个人信息的基本概念及范围进行了界定，对个人信息收集、使用、转移等环节的安全要求加以明确。《网络安全法》第三十七条、《个人信息和重要数据出境安全评估指南（征求意见稿）》、《信息安全技术 数据出境安全评估指南（征求意见稿）》等法律法规中对于拟出境的个人信息和重要数据的安全做出了在本地存储的要求，当确有必要出境时，需根据法定程序进行安全评估。

数据安全对于网络运营者的重要性不言而喻，对于大数据、云计算等新一代信息技术的长久发展更是起到基础性的作用。因此，国内外网络运营者也已经开始在日常的安全维护中通过重视系统漏洞修复，公布漏洞悬赏计划鼓励“白帽子”进行漏洞挖掘，从而改善自身系统安全性，保障数据安全。Facebook、谷歌、雅虎、微软，我国的360、阿里巴巴、百度都公布过相关的漏洞悬赏计划。

## 态势五：重视国际网络空间治理， 构建网络空间命运共同体

网络技术的发展带动了社会生产的变革，改变了人与人之间传统的沟通交流与探索世界的方式。一方面，在世界各国合作日益密切，经济全球化、文化多样性深入发展的背景下，信息通信技术的蓬勃发展将人们带入信息革命的新时代，工业控制系统、微电子、软件技术等进一步解放和发展了生产力，无人驾驶汽车、无人机、物联网等技术使人们走得更远、看得更清，信息革命在一定程度上打破了传统地域的限制，将世界各国人民的发展与安全紧紧地联系在一起。另一方面，网络也带来了新的问题与挑战。网络主权共识如何达成，网络领域发展水平不均、规则缺失等问题日益凸显，国家和地区间的“数字鸿沟”不断拉大。跨国网络犯罪、网络恐怖

主义治理、网络强国滥用信息技术攻击他国基础设施、进行大规模网络监控的事实不容忽视。在网络社会中，任何一个国家都难以独善其身，国际社会应在相互尊重的基础上，开展对话与合作，以规则为基础实现网络空间全球治理。

2016 年 10 月，美国商务部下属机构国家电信和信息局将互联网域名管理权交给位于加利福尼亚州的“互联网名称与数字地址分配机构”，两者之间的授权管理合同于当日自然失效，不再续签。至此，美政府理论上不再拥有该领域的主导权，标志着互联网迈出走向全球共治的重要一步。除此之外，近年来，美国与欧盟之前从“安全港”协议到“隐私盾”协议的博弈，亚洲太平洋经济合作组织（Asia-Pacific Economic Cooperation, APEC）跨境隐私规则体系成员的不断加入，上海合作组织成员进一步开展打击网络恐怖主义国际合作，中俄进一步深化全面战略协作伙伴关系、首轮中美外交安全对话等事件的发生，也充分说明世界各国，不论大小，都在积极参与网络空间的国家合作。在我国公布的《网络空间国际合作战略》中，也明确表示中国致力于维护网络空间和平安全，以及在国家主权基础上构建公正合理的网络空间国际秩序，并积极推动和巩固在此方面的国际共识。

在国际经济交往过程中，大型互联网企业的发展也在一定程度上促进着网络空间命运共同体的构建。例如，苹果近期宣布将在我国建造数据中心，我国 360、阿里巴巴、京东等企业向国际市场的拓展都能够有效助推我国更好地参与网络空间的国际治理。

总而言之，在当前的国内外网络安全态势中，总体上呈现机遇与挑战并存的局面。网络给政治、经济、文化、外交等领域带来的价值已经充分体现，并且伴随着人工智能、虚拟现实等新兴技术的发展成熟，这一价值会进一步得到拓展，信息革命带来的益处正在普惠世界各国人民。但与此同时，风险也接踵而至。网络谣言、恐怖主义的甚嚣尘上，网络犯罪的肆虐，黑色产业链的不断蔓延，网络攻击的频发及关键信息基础设施保护的迫切性日益凸显，网络资源分布不均，“数字鸿沟”的不断拉大使得网络空间的国际竞争不断加剧。在此背景下，各国在出台立法，完善信息内容治理，惩治网络恐怖主义和网络犯罪，发展核心技术的同时，积极参与网络空间的国际合作，加强国际信息共享与执法协助，致力于构建网络空间命运共同体。

# 国外网络安全立法与事件

从 1946 年世界上第一台电子计算机问世开始，在短短数十年内，计算机从价格昂贵、数量稀少、体积巨大的科研军事设备发展为普通大众社会生活的必备品。网络也经历了从 20 世纪 60 年代早期第一代远程终端连接，即仅提供终端和主机之间通信的计算机网络；到 20 世纪 60 年代中期第二代局域网阶段，即实现多个主机互联，实现计算机和计算机之间的通信；之后发展到第三代计算机网络互联阶段，能够实现不同厂家生产的计算机之间的互联；现已进入第四代信息高速公路阶段，网络使用覆盖社会生活的方方面面，为人们进行高速、多业务、大数据量的信息处理。

## 第一节 网络安全规制形式

随着新技术的发展和普及，网络在个人生产生活、社会及国家运行方面所占的比重越来越大。为了维护社会安定和国家安全，世界各国通过各种不同形式对涉及网络领域的安全进行相应的规制和保障。

最直接的是各国制定与网络安全相关的国内部门法，如美国的《网络安全法案》、德国的《IT 安全法》、克罗地亚的《信息安全法》、捷克共和国的《网络安全法》、匈牙利的《中央和地方政府机构电子信息安全法》，以及我国最新颁布的

《网络安全法》等。这样对网络安全管理事务直接立法进行规制的形式能够较为系统地对本国的网络安全管理进行设计。由于国内部门法通常结构较为紧凑、完整，对于涉及网络安全保障各方的责任义务划分明确，所以能够切实对网络安全保障工作起到指导作用。

除了制定相应部门法之外，很多国家和地区选择制定网络安全战略等政策性文件以便进行网络安全规制，如美国、俄罗斯、欧盟、英国、法国、德国等都推出了他们的国家网络安全战略，或者在国家安全战略中专门列出网络安全保障章节。我国也在 2016 年发布了国家网络安全战略，并在 2017 年发布国际网络合作战略。这样的规制方式相较于法律法规更加提纲挈领、且易于更新，符合网络这一特殊领域的管制需求。由于技术的高速更新和不可预知性，所以进行方向性和纲领性的战略文件制定并及时进行增补是网络管制的有效形式。

第二节 国外主要国家及地区网络安全立法情况概述

自计算机和网络诞生之初，安全问题就相伴而生，飞速的技术和其他应用形式的更迭，使得网络空间安全形势也越发严峻并逐渐上升为影响国家和社会安定的全局性问题。目前全世界 90 多个国家均已制定、颁布针对网络安全及相关问题的管控措施和专门立法。对于网络空间进行科学的治理已经成为世界各国的共同态度。美国、俄罗斯、英国、德国、澳大利亚、新加坡、印度等国家都制定了专门的国内立法，欧盟等国际组织也积极推动相关决议维护网络空间安全秩序（见表 2-1），而我国也在经历了长期的积累和充足的研讨后制定、发布了《网络安全法》，正式进入网络治理的法治时代。

表 2-1 国外主要国家及国际组织网络安全政策和法律文件摘要

国家	网络安全政策及立法名称	年份（年）
美国	网络空间政策审查（Cyberspace Policy Review）	2009
	国际网络战略网络世界的繁荣、安全和开放 （International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World）	2011



续表

国家	网络安全政策及立法名称	年份（年）
美国	改善关键基础设施网络安全的行政令 (Improving Critical Infrastructure Cybersecurity)	2013
	2014 年网络安全增强法案 (Cybersecurity Enhancement Act of 2014)	2014
	2014 年国家网络安全保护法 (National Cybersecurity Protection Act of 2014)	2014
	改进关键基础设施网络安全草案 (Draft Strategy for Improving Critical Infrastructure Cybersecurity)	2014
	国家安全战略 (National Security Strategy)	2015
	国防部网络战略 (The Department of Defence Cyber Strategy)	2015
	2015 年网络安全法案 (Cybersecurity Act of 2015)	2015
	增强联邦政府网络与关键基础设施网络安全的行政令 (Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure)	2017
俄罗斯	关于俄罗斯联邦武装力量在信息空间活动的概念性观点 (Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space)	2011
	俄罗斯联邦国际信息安全领域国家政策基本原则 (Basic Principles for State Policy of the Russian Federation in the Field of International Information Security)	2013
	俄罗斯联邦外交政策理念 (Concept of the Foreign Policy of the Russian Federation)	2013
	俄罗斯联邦军事理论 (Military Doctrine of the Russian Federation)	2014
	俄罗斯网络安全战略概念—进行中的草案 (Concept of Russia's Cyber Security Strategy - draft underway)	2014
	俄罗斯联邦国家安全战略 (National Security Strategy of the Russian Federation)	2015
	续展进行中——俄罗斯联邦信息安全理论 (Renewal underway, Information Security Doctrine of the Russian Federation)	2016
欧盟	欧盟网络安全战略：公开、可靠和安全的网络空间 (Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace)	2013
	欧盟网络防御政策框架 (EU Cyber Defence Policy Framework)	2014

续表

国家	网络安全政策及立法名称	年份（年）
欧盟	欧洲安全议程 (The European Agenda on Security)	2015
	欧洲议会和欧盟理事会关于自然人个人数据处理和数据自由流动保护，并废除 95/46/ EC 号指令的第 2016/680 号条例（通用数据保护条例） [Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) ]	2016
	欧盟网络与信息系统安全指令 (The Directive on Security of Network and Information Systems)	2016
	欧洲议会和欧盟理事会关于欧盟高级别网络和信息系统安全措施的第 2016/1148 号指令 [Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union]	2016
英国	战略防务与安全审查——在不确定的时代下建立一个安全的英国 (A Strong Britain in an Age of Uncertainty: The National Security Strategy)	2010
	紧急通信与互联网数据保留法案 (Data Retention and Investigatory Powers Act)	2014
	2016—2021 年国家网络安全战略 (National Cyber Security Strategy 2016—2021)	2016
澳大利亚	强大和安全，澳大利亚国家安全战略 (Strong and Secure. A Strategy for Australia's National Security)	2013
	澳大利亚网络安全战略 (Australia's Cyber Security Strategy)	2016
	2016 年国防白皮书（2016 Defence White Paper）	2016
印度	国家网络安全政策（National Cyber Security Policy）	2013
以色列	提高国家网络空间能力第 3611 次决议 (Advancing National Cyberspace Capabilities, Government Resolution No. 3611)	2011
	推进国家监管和网络安全政府领导第 2443 号决议 (Advancing National Regulation and Governmental Leadership in Cyber Security, Government Resolution No. 2443)	2015
	推进国家网络安全防范第 2444 号决议 (Advancing the National Preparedness for Cyber Security, Government Resolution No. 2444)	2015

续表		
国家	网络安全政策及立法名称	年份（年）
日本	网络安全战略——迈向世界领先的、弹性的、充满活力的网络空间 （Cybersecurity Strategy-Toward a World-Leading, Resilient and Vigorous Cyberspace）	2013
	网络安全国际战略—网络安全倡议 （International Strategy on Cybersecurity - j-Initiative for Cybersecurity）	2013
	日本防卫计划（Japan Defense）	2015
	网络安全策略（Cyber Security Strategy）	2015
	关键信息基础设施保护基本政策 （Basic Policy of Critical Information Infrastructure Protection）	2015
新加坡	2018 年国家网络安全总体规划 （National Cyber Security Masterplan 2018）	2013
	2018 年国家网络安全总体规划纲要 （Factsheet on National Cyber Security Masterplan 2018 Cyber security strategy）	2016
越南	密码法（Law on cipher）	2011
	网络信息安全法 （Vietnam’s 2015 Cyber Information Security Law）	2015

一、美国法

美国是全球网络技术发源地，在新技术方面占有绝对优势地位，同时其颁布的网络信息安全相关法案也是最多的，据不完全统计至今共计高达 130 余部，具体涉及计算机系统的运行标准、信息处理的方法和具体技术操作、不同群体的网络权益等领域，规制了行业准入、电话通信、数据保护、消费者保护、版权保护等方面，对破坏网络基础设施的犯罪行为也制定了严格的惩处标准。

在网络信息安全方面，美国有严格的数据信息保密法，规定公民隐私权不容侵犯且使用者有义务对信息进行保密等。而“9·11 事件”的发生直接导致美国将立法重点放在保护国家安全和打击恐怖主义之上，对于网络空间的管辖也必须充分考虑安全可控性。例如，2001 年通过的《爱国者法案》，明确授予美国国家安全局以保护国家安全，打击恐怖主义为目的收集调查任意美国民众电话记录和数据记录的权利，这无疑是对网络空间管控的极大强化。近几年的《国土安全法

案》和《国防授权法案》也都对网络部分的国家部门设置、职责划分和国家预算进行不断的更新和细化。

除了国家层面外，在社会安全层面美国也进行了系统化的网络安全立法。例如，2010 年美国审议了《2010 年网络安全加强法案》，该法案的目的是加强网络安全的研究与发展，推进网络安全技术标准制定。2015 年美国审议了《美国创新与竞争力法案》，这项法案要求国家科学基金会发布并定期更新其工作人员和政策指导意见，研究满足未来网络安全需求的信息系统，并制定流程用以研究能够满足未来网络安全需求的加密标准和准则。

此外，美国还高度重视关键基础设施的安全保护，以及国家网络安全审查制度建设。例如，2017 年特朗普政府签发的《增强联邦政府网络与关键性基础设施网络安全》行政令。这项行政令要求采取一系列措施来增强联邦政府及关键基础设施的网络安全，并按联邦政府、关键基础设施和国家三个领域来规定将采取的增强网络安全的措施。在关键基础设施网络安全方面，要求按关键基础设施名单进行评估，并提交网络安全风险评估报告，之后每年重新评估并提交一次评估报告。该项行政令还要求政府机构为重要行业的私有部门和运营商（例如，银行、通信和水电等公共事业）提供更多帮助。

## 二、俄罗斯法

在网络安全日趋重要的新形势下，俄罗斯一直非常注重网络防护。《俄罗斯联邦宪法》已经将信息安全纳入了国家安全管理范围，在此基础上制定颁布了《俄罗斯联邦信息、信息化和信息网络保护法》，以此规范俄互联网行为。除此之外，俄罗斯针对信息安全还进行了部分专项立法，从上到下形成了较为完备的多层级信息安全法律体系。

俄联邦安全局的统计数据显示，俄罗斯总统办公厅、国家杜马、联邦委员会网站每天遭受黑客攻击达 1 万余次，俄计算机用户面临来自互联网的风险水平连续数年高居全球首位。而在“棱镜门”事件中，美国对各国进行网络攻击及监视范围之广也让俄罗斯政府及军方大为警觉。因此，提高网络安全应对能力成为俄政府和军方近年来的重要议题。2013 年 1 月普京签署总统令，要求俄联邦安全局

建立国家计算机信息安全机制来监测、防范和消除计算机信息隐患，具体内容包括评估国家信息安全形势、保障重要信息基础设施的安全、对计算机安全事故进行鉴定、建立计算机攻击资料库等。

俄罗斯在信息安全立法方面较为重视纲领性文件的作用。先后出台了《俄罗斯网络立法构想》、《俄罗斯联邦信息和信息化领域立法发展构想》、《信息安全学说》等纲领性文件，在这些指导性文件和纲领性文件的指导下，涉及各领域的网络安全立法工作得以有序进行，并通过了一系列包括《俄联邦计算机软件和数据库法律保护法》、《俄联邦保密法》、《俄联邦著作权法》、《个人信息法》、《电子合同法》、《电子商务法》、《电子数字签名法》、《产品和服务认证法》、《信息保护设备认证法》等法律。

2017年7月，俄罗斯议会上院通过了一揽子政府法案，以保护关键信息基础设施免遭网络攻击，其中明确关键基础设施包括政府数字系统和电信网络、国防行业技术流程自动化控制系统、医疗保健、交通、通信、金融、能源、核、航空航天等行业。法律同时规定，创建恶意软件，并对关键基础设施造成严重损害者可能被判处长达10年的监禁。

### 三、欧盟法

欧盟是较早拥有网络安全管制意识的国际组织之一，多年的立法实践过程使其在网络安全体系建设方面成效显著。早在2001年欧盟就提出了“网络和信息安全相关建议”，并在随后的2004年成立欧盟网络和信息安全局，收集分析欧洲网络安全事件数据并提高欧盟各国应对信息安全风险的能力，协调信息安全领域各个参与主体活动，协助各国计算机应急响应组织的各项活动。

在个人数据保护立法方面，欧盟立法机构的态度存在较为明显的转变。2006年3月马德里和伦敦公交系统遭遇恐怖袭击后，欧盟颁布了《数据保留指令》，该指令要求电信公司将欧盟公民的通信数据保留6个月到两年。但随着“棱镜门”曝光及一系列个人数据泄露和监听行为的披露，2014年4月8日，欧洲法院裁定《数据保留指令》无效，理由是该项指令允许电信公司对使用者的日常生活习惯进行跟踪，侵犯了公民人权。

2016年7月6日，欧盟立法机构正式通过首部网络安全法《网络与信息系统安全指令》，旨在加强基础服务运营者、数字服务提供者的网络与信息系统之安全，要求这两者履行网络风险管理、网络安全事故应对与通知等义务。此外，该法要求成员制定网络安全国家战略，要求加强成员间合作与国际合作，要求在网络安全技术研发方面加大资金投入与支持力度。

在实践方面，2013年1月，欧盟委员会在荷兰首都海牙正式成立欧洲网络犯罪中心，以应对欧洲日益增加的网络犯罪案件。网络犯罪中心连通所有欧盟警务部门的网络，整合欧盟各国的资源和信息，支持犯罪调查，从而在欧盟层面找到解决方案，维护一个自由、开放和安全的互联网，保护欧洲民众和企业不受网络犯罪的威胁。2013年4月，欧洲部分私人网络安全公司联合成立了欧洲网络安全小组，通过联合600多名网络安全专家针对问题做出快速有效的反应，建立伙伴关系。同时利用“一线经验”优势，在网络防御政策、风险预防、跨境信息共享等问题上向政府、企业和监管机构提供更有效和实用的建议。

## 四、英国法

目前，英国的网络安全立法较为完整。英国不仅通过国家网络安全战略等形式对网络安全治理方向进行规制，还在关键信息基础设施保护、个人信息安全、跨境数据流动等方面进行专门立法。除此之外的一系列实践措施也有助于政府、企业、民众相互配合，完善互联网的治理和管控。

2000年，英国制定了《通信监控权法》，规定在法定程序条件下，为维护公众的通信自由和安全及国家利益，可以动用皇家警察和网络警察。该法规定了对网上信息的监控。“为国家安全或为保护英国的经济利益”等目的，可截收某些信息，或者强制性公开某些信息。2001年实施的《调查权管理法》，要求所有的网络服务商均要通过政府技术协助中心发送数据。2014年7月，英国政府召开特别内阁会议，通过了《紧急通信与互联网数据保留法案》，该法案允许警察和安全部门获得电信及互联网公司用户数据的应急法案，旨在进一步打击犯罪与恐怖主义活动。

2009年6月，英国出台了首个国家网络安全战略，宣布成立“网络安全办公室”和“网络安全运行中心”，提出建立新的网络管理机构的具体措施，以促进

产业发展和维护网络安全。2010年10月，英国政府发布了《战略防务与安全审查——在不确定的时代下建立一个安全的英国》，将恶意网络攻击与国际恐怖主义、重大事故或自然灾害，以及涉及英国的国际军事危机共同列入安全威胁的最高级别，建议启动为期四年、总额达6.5亿英镑的国家网络安全计划。2011年11月，英国公布新的《网络安全战略》，表示将建立更加可信和适应性更强的数字环境，以实现经济繁荣，保护国家安全及公众的生活所需；并将加强政府与私有部门的合作，共同创造安全的网络环境和良好的商业环境。近年来，英国愈加注重技术人才的储备，在2014—2015年，英国分别在多所大学里设立专家课程并提出“网络安全学徒计划”，旨在号召青年人加入网络信息安全领域。

## 五、澳大利亚法

澳大利亚有着良好的信息安全保护传统，其信息安全立法可谓走在世界前列。早在1988年，澳大利亚就专门制定了保护个人信息的《隐私法》。随着通信技术的发展，澳大利亚政府及各部门制定了一系列与信息安全有关的法律、标准和指南，包括《电信传输法》、《反垃圾邮件法》、《数字保护法》、《信息安全手册》等，修订了《刑法》，以适应打击新型网络犯罪。2000年，澳大利亚政府发布信息安全风险管理指南。2001年，发布“保护国家信息基础设施政策”，即政府信息安全行动计划，用以对澳大利亚的关键基础设施进行保护。此外，澳大利亚标准局还制定和采纳了一系列信息安全标准，主要包括信息安全管理标准、澳大利亚和新西兰信息安全管理标准、澳大利亚联邦政府IT安全手册、IT安全管理的信息技术指南等。政府部门都被要求遵循这些标准，执行情况由国家审计署进行审查。

2009年澳大利亚政府发布《网络安全战略》，从此将网络安全提升到国家战略的高度。该战略详细描述了澳大利亚政府将如何保护经济组织、关键基础设施、政府机构、企业和家庭用户，使之免受网络威胁；并确立了国家领导、责任共担、伙伴关系、积极的国际参与、风险管理和保护价值观六大指导原则。该战略还提出了信息安全三大战略目标：一是让澳大利亚所有公民都意识到网络风险，确保其计算机安全，并采取行动确保其身份信息、隐私和网上金融的安全；二是让澳大利亚企业能利用安全、灵活的信息和通信技术，确保自身操作和客户身份信息与隐私的完

整性；三是让澳大利亚政府能确保其信息与通信技术是安全的且对风险有抵抗力。

2016 年，澳大利亚政府公布了新的《澳大利亚网络安全战略》。此安全战略的重点是提升澳大利亚在网络环境中的保护能力，以及提高对网络恶意行为的抵抗力。澳大利亚政府计划拨款 2.3 亿澳元加强网络安全，并为澳大利亚联邦警署、犯罪委员会和通信局等部门聘请网络安全专家。同时，澳大利亚制定了一系列与信息安全有关的法律、标准和指南，包括《广播服务法》、《反垃圾邮件法》、《互联网内容法规》、《数字保护法》等，规定各社会主体对网络安全承担的责任和义务。政府部门和司法机构也必须根据这些法律采取管理措施，惩治破坏网络安全的行为。

澳政府还积极开展网络安全教育，提高全民网络风险意识。例如，免费在计算机上安装软件，屏蔽不良网站，建立青少年网络安全保护公益组织，并为公众投诉非法的互联网内容设立了举报投诉机制。

## 六、新加坡法

新加坡的网络安全指数位列全球第一位，这得益于其严格的网络管理体制和超前的网络治理思维。早在 1997 年，新加坡就成立了国家计算机应急响应队伍。2005 年，新加坡发布了该国首个《信息安全总体规划（2005—2007 年）》，旨在保护国家网络环境，建立公共领域面对网络威胁时响应和处理的基本能力。随后，在 2008 年和 2013 年，新加坡又先后推出了第二、第三部《信息安全总体规划》。尤其是第三部《信息安全总体规划》，旨在使新加坡在 2018 年之前发展成为值得信赖并健全的资讯通信枢纽。

《国内安全法》是新加坡国家安全的基础性法规，其在管理网络安全方面规定了禁止性文件与禁止性出版物，互联网服务提供商的报告义务，以及为了维护国家安全，国家机关拥有的调查权与执法权。《互联网操作规则》明确规定互联网服务提供者和内容提供商应承担自审义务，配合政府的要求对网络内容自行审查，发现违法信息时应及时举报，且有义务协助政府屏蔽或删除非法内容。同时，新加坡还将上百个政治性网站列入禁访者清单，不遵守规定的网络服务供应将被吊销执照或罚款，私下访问者也会受到刑罚。政府还鼓励服务供应商开发推广“家庭上网系统”，协助用户过滤不适宜看到的内容。



在网络安全实践方面，新加坡也做出了许多创新性尝试。2009年新加坡成立了资讯通信科技安全局，主要职责包括监管和保障关键信息基础设施领域的网络安全问题，保护新加坡免受网络攻击和网络间谍活动的威胁。随后的2015年4月，新加坡又成立了网络安全局，以统筹政府各部门的网络安全事宜应对网络安全威胁日益增加、个人信息泄露事件接连发生的情况。

2016年，随着新加坡提出打造数字化智能国家的计划，相应对网络和数字科技的依赖与日俱增，新加坡对网络安全越发重视，推出了《新加坡网络安全策略》，旨在推动政府机构、网络行业、专家学者和主要服务业者等各利益方共同努力来打击网络犯罪。新加坡网络安全局将成立网络安全学院，通过相关培训提高政府机构及关键信息基础设施网络安全人员的技能水平，确保新加坡有足够的 ability 更好地应对网络袭击。网安局也会连同资讯通信专才协会和其他机构推出网络安全奖，肯定杰出网安专家、机构，以及学生对本地网安系统做出的贡献。

2017年，新加坡发布了《网络安全法案（草案）》，该法案聚焦应对网络安全威胁和事故、维护关键信息基础设施、促进信息的分享、管制网络安全行业四方面。它将授权新加坡网络安全局在发生网络袭击时立即展开调查，并要求受影响单位提供事故报告和其他关键资料，其效力将凌驾于新加坡的资料与隐私保护条例之上。

## 七、日本法

在亚洲国家之中，日本网络技术发展起点高、速度快，网络规制意识成型较早。在1988年日本就制定了《关于保护行政机关所持有之个人信息法律》；2003年5月颁布了日本《个人信息保护法》，并相继制定、颁布了针对行政机关、独立行政法人等持有个人信息机关的多部法律。

在消灭垃圾邮件、计算机病毒及保护网民隐私信息方面，日本也有明确的法律。日本2011年对《刑法》进行了部分修正，要求网络运营商原则上保存用户30天上网和通信记录，根据必要还可以再延长30天。在网络安全方面，2013年6月10日，日本正式发布《日本网络安全战略》，提出了创建“领先世界的强大而有活力的网络空间”，实现“网络安全立国”的目标。

2014年11月6日，日本国会众议院表决通过《网络安全基本法》，规定电力、

金融等重要社会基础设施运营商、网络相关企业、地方自治体等有义务配合网络安全相关举措或提供相关情报，此举旨在加强日本政府与民间在网络安全领域的协调和运用，更好应对网络攻击。该法还规定，日本政府将新设以内阁官房长官为首的“网络安全战略本部”，协调各政府部门的网络安全对策，与日本国家安全保障会议、IT 综合战略本部等其他相关机构加强合作。

在实践方面，日本还采取了完善信息安全机构、扩充网络安全力量、健全信息安全保障机制、研发网络安全技术、举行信息安全演习、举办黑客技术比赛、严厉打击网络违法行为、广泛开展交流合作等一系列举措，加强信息网络安全建设。

## 八、印度法

印度一直非常重视网络监管，惩罚措施也相当严厉。印度是世界上为数不多专门为信息技术立法的国家之一。早在 2000 年，印度就颁布了《信息技术法》，规定了八类行为构成“破坏计算机和计算机系统”犯罪，一经查实，犯罪者要负担的民事赔偿金额最高可达 1 000 万卢比。除此之外，该法还涉及刑事、行政管理、电子商务等内容，为该国网络监管提供了法律框架。印度的刑法典、刑事诉讼法、银行法、证据法也进行了相应的修改以适应信息网络发展的要求。

2007 年，印度政府下决心将网络监管系统化。2008 年孟买连环恐怖袭击事件的发生，促使印度政府重新修订《信息技术法》，特别将移动通信纳入监管范畴。2011 年印度政府进一步修订了《信息技术法》，重点加大对网站的规范管理，并规定印度政府有关部门有权查封可疑网站、删除不良内容。

在实践方面，印度政府成立了印度数据安全委员会，专门针对日益增多的网络数据安全问题提供权威监测和管理方法。印度当局建立了针对网络犯罪的警察局和计算机犯罪分析实验室等专门机构，中央调查局也开始与美国等一些国家的安全机构共享情报，共同打击跨国网络犯罪。

## 九、以色列法

1995 年 4 月，以色列政府正式成立了名为“计算机系统和信息安全审查顾问

委员会”的职能机构，组织以国防部门职业军人为主的专业队伍，为政府研究设计信息安全领域的管理标准，承担 IT 系统的安全审计，并就计算机敏感领域的安全管理提供对策性建议。

2002 年以后，以色列的内外安全形势发生了较大变化。一方面，在国内安全环境上，以色列民众和关键基础设施日益遭受巴勒斯坦抵抗组织的袭击，并且出现了利用移动电话、互联网络等 IT 技术组织、协调恐怖行动的苗头；另一方面，在国际安全环境上，针对国家关键基础设施的网络攻击初现端倪，特别是 2007—2008 年所发生的爱沙尼亚和格鲁吉亚网络被攻事件给以色列政府敲响了警钟。在这种情况下，以色列国家安全委员会于 2002 年 12 月 11 日出台了名为《以色列信息化系统保护职责》的“B/84 号特别决议”，这是以色列正式公布的首例网络安全政策。该政策与美国 2002 年所颁布的《关键基础设施信息保护法》几乎处于同一时期，这使得以色列迅速跻身于全球关键基础设施保护的先驱国家行列。在“B/84 号特别决议”中，以色列对关键基础设施的相关概念进行了清晰的定义，并明确了未来网络安全政策的实施手段和建设目标，同时还表示关键基础设施的保护工作需由使用者和监管者共同承担，实施义务上的分摊协作，发挥监管组织上的专项职责。

2010 年，以色列参照美国发布《网络安全评估报告》的方式，对国家现有网络安全整体状况进行了全面评估。启动此次评估项目的主要目的是进一步摸清以色列网络政策的实施效果、预判网络安全的风险挑战，进而为下一阶段以色列网络空间优势能力的提升奠定扎实的基础。经过“国家网络计划”的评估诊断后，以色列政府于 2011 年 8 月 7 日正式公布了关于推动国家网络空间能力的“3611 决议”，即《2011 以色列国家网络战略》。该战略采用了“国家网络计划”中的多项政策建议，提出要强化以色列国内各领域网络安全设施的防护水平，鼓励政府部门、学术界、工商界和企业界等单位协同攻关、通力合作，推动以色列网络空间能力建设，改进国家网络安全治理水平，进而确保以色列全球五大网络强国的优势地位。

## 十、越南法

尽管越南在国际电信联盟发布的《2017 年全球网络安全指数》报告中位于东南亚国家网络安全排名的较后位置，但越南国家和政府已经逐渐意识到网络所带

来的机遇及应对相关安全威胁的重要性，先后在 2011 年和 2015 年颁布了《密码法》和《网络信息安全法》，在网络治理规范化、系统化的道路上进行不断探索。

2011 年，越南颁布了《密码法》，从整体上规定了国家密码活动及其参与人员的权利、义务和责任，并重点关注国家机密领域的密码管理。这一举措在当时的东南亚地区属于先进的立法实践。

2015 年年初，越南《信息安全法（草案）》被更名为《网络信息安全法（草案）》，其于 2015 年 11 月 19 日上午由越南国会表决通过，并于 2016 年 7 月 1 日起生效。该法规定了机关、组织和个人在保护网络信息安全过程中的网络信息安全活动、权利和义务、民用密码、网络信息安全的技术标准与规范、信息安全业务、网络信息安全的人员发展、国家网络信息安全管理等内容。该法普遍适用于任何越南机关、组织或个人，以及越南境内直接参与或从事越南网络信息安全相关活动的外国组织和个人。从内容上来看，这部《网络信息安全法》是越南国家和政府在面对来自互联网安全挑战时制定的一部较为完整的“参考答案”；从已有的密码管理和使用领域上来看，它在一定程度上是对越南《密码法》的补充和细化。

### 第三节 国外网络安全事件概要

#### 一、针对关键信息基础设施的攻击

##### （一）爱沙尼亚遭受大规模网络攻击事件

爱沙尼亚是人口仅 140 万的小国，但被认作网络化最彻底、网络办公发展最迅猛的欧洲国家。人们投票、交税、转账几乎全部使用网络完成，连停车费一般都用手机短信息交纳。不难想象，爱沙尼亚对互联网的依赖程度之大。而爱沙尼亚也是历史上第一个政府和关键基础设施经历大规模网络攻击的国家。该事件发生在 2007 年 4 月到 5 月的 3 个星期里，在这期间爱沙尼亚遭受了旷日持久的网络攻击，大量的来自全世界的僵尸网络瘫痪了该国的互联网。其中大多数都是通过汹涌而来的在线请求淹没服务器的，让服务器无法接收新的通信，从而拒绝服务。

攻击的主要目标是爱沙尼亚总统、政府部门和一些新闻组织的网站，一些银行也遭受了攻击。在这个高度网络化的国家，人们的生活安全受到了严重威胁。由于银行服务器崩溃，大量计算机遭恶意软件侵入，所有民众日常消费或其他在线金融行为都无法正常进行。爱沙尼亚政府为了终结这次网络攻击，不得不采取了切断互联网这样的极端做法。这标志着一种新的、难以追踪、影响国际安全、没有固定模式的威胁的开始。

## （二）伊朗核电站遭袭事件

2010年9月，伊朗政府宣布，纳坦兹铀浓缩基地至少有3万台计算机受病毒感染，1/5的离心机瘫痪，病毒攻击目标直指核设施。由于被病毒感染，监控人员看到的是正常画面，而实际上离心机在失控情况下不断加速而最终损毁。造成这样严重后果的病毒被称为“震网”，其包含空前复杂的恶意代码，是一种典型的计算机病毒，能自我复制，并将副本通过网络传输，任何一台个人计算机只要和染毒计算机相连，就能自动将病毒传播给其他与之相连的计算机，最后造成大量网络流量的连锁效应，导致整个网络系统瘫痪。“震网”主要通过U盘和局域网进行传播，是第一个利用Windows“零日漏洞”，专门针对工业控制系统发动攻击的恶意软件，能够攻击石油运输管道、发电厂、大型通信设施、机场等多种工业和民用基础设施，被称为“网络导弹”。这预示着网络战已发展到以破坏硬件为目的的新阶段。

## （三）乌克兰电网遭黑客攻击事件

2015年12月23日，乌克兰首都基辅部分地区和乌克兰西部的140万名居民突然发现家中停电。这次停电不是因为电力短缺，而是遭到了黑客攻击。黑客利用欺骗手段让电力公司员工下载了一款恶意软件“Black Energy”。当天，黑客攻击了约60座变电站。黑客首先操作恶意软件将电力公司的主控计算机与变电站断开，随后又在系统中植入病毒，让计算机全体瘫痪。与此同时，黑客还对电力公司的电话通信进行了干扰，导致受到停电影响的居民无法和电力公司进行联系。这是有史以来首次导致停电的网络攻击，此次针对工控系统的攻击引起世界范围的高度关注。

## 二、网络监听及间谍行动

### （一）“棱镜门”曝光

2013 年 6 月 5 日，美国前中情局职员爱德华·斯诺顿披露给媒体两份绝密资料，一份资料称：美国国家安全局有一项代号为“棱镜”的秘密项目，要求电信巨头威瑞森公司必须每天上交数百万名用户的通话记录。另一份资料更加惊人，显示美国国家安全局和联邦调查局通过进入微软、谷歌、苹果等九大网络巨头的服务器，监控美国公民的电子邮件、聊天记录等秘密资料。在此后的时间里，一连串的新闻报道更加印证了许多隐私倡导者担心很久的问题，即全球的网络、电子通信，正处在以美国政府为主导的监控之下。随着事件的进一步发酵，各项证据证明美国的监控目标还包括世界多国领导人及多个政府部门和银行。这项大规模监听行动的曝光引发了一系列后续反应，包括欧盟在内的多个国际组织和受监听国家表示将重新审视与美国的数据共享协议；美国国内民权组织也提出了针对侵犯公民言论自由权和隐私权方面的政府违宪诉讼。

### （二）网络间谍程序——红色十月

2015 年，某安全研究机构证实了称为“红色十月”的计算机病毒的存在，这一病毒专门攻击全球各国政府机构和外交使团、从事网络间谍活动，目前已有 50 多个国家的网络遭到它的攻击。“红色十月”是近年来曝光的最复杂网络间谍平台，它有超过 1 000 个独立模块，可以根据被感染计算机和目标用户定制模块配置。它首先收集被感染机器的一般信息，包括浏览历史和储存的密码等，然后攻击者评估其价值决定下一步安装哪些模块，它有专门的模块可以窃取证书获取账号密码；提取 Outlook 和 Thunderbird 等邮件客户端存储的信息和数据；窃取连接的 USB 设备数据；记录按键；扫描本地网络主机，感染其他计算机；从连接的智能手机中下载有价值的信息，如联系人信息等。

### （三）网站数据和个人信息泄露事件

#### 1. 土耳其重大数据泄露事件

2016 年 4 月 3 日，土耳其爆发重大数据泄露事件，近 5 000 万名土耳其公民

的个人信息牵涉其中，包括姓名、身份证号、父母名字、住址等一连串敏感信息被黑客打包放在芬兰某 IP 地址下，人们可通过 P2P 任意下载他们感兴趣的数据。同时，为了证明这些被盗取数据的真实性，黑客特地公布了土耳其现任总统埃尔多安的个人信息以作示范。

## 2. 黑客组织“Peace”攻击多家公司造成数据泄露事件

2016 年 5 月，位于美国纽约的轻博客网站 Tumblr 被证实卷入一起数据泄露事件，涉及的邮箱账号和密码达 65 469 298 个。事实上，该泄露事件早在 2013 年就开始持续发酵，但直到 2016 年 Tumblr 才发现了漏洞所在。据对 Tumblr 发起网络攻击的黑客组织“Peace”称，Tumblr 在用户数据中使用的是 SHA-1 算法，其安全性能并不高，也正因为如此才成为 Peace 攻击的目标。

2016 年 5 月 19 日，美国职业社交网站 LinkedIn 宣布，名叫“Peace”的黑客组织在黑市上以 5 个比特币（约合 2 200 美元）的售价公开销售 1.67 亿个领英用户登录信息。据了解，这些数据来自 2012 年 LinkedIn 发生的一次大范围的数据泄露事件，其中包含 1.17 亿条数据，既包括电子邮件，也包括密码。事后，LinkedIn 已经给用户发送了电子邮件要求更改密码。

2016 年 6 月初，同样是代号为“Peace”的黑客称已经拿到了全球第二大社交网站 MySpace 的 3.6 亿个用户账号及 4.27 亿个密码，并且在暗网上以 6 个比特币（合 2 800 美元）的价格公开出售。至于如何窃取到如此庞大的数据，MySpace 与黑客方面均未透露。

## 3. 雅虎账户数据泄露事件

雅虎遭受了近年来最大的数据泄露事件。2016 年 9 月，雅虎宣布发现 2014 年年底的一次数据泄露影响到超过 5 亿个用户账户。该事件导致部分用户账户信息泄露，包括姓名、电子邮件地址、电话号码、出生日期、散列密码、一些加密或未加密的安全问题和答案。雅虎表示，他们认为该事件背后是国家级的攻击。就在几个月之后，雅虎宣布遭遇第二次更大规模的攻击，影响到 10 亿个用户账户。这次事件揭示了即使是世界上最大的公司也无法避免巨大的数据泄露，而这种巨量数据泄露事件会影响数百万名消费者。现代国家、政府和企业需要全面的、全方位的数据保护政策和方式。

# 我国网络安全立法与事件

在接入国际互联网的 20 余年里,我国一直致力于完善对网络安全领域的监管与立法工作。经济基础决定上层建筑的原理同样体现在我国网络安全立法实践的历史过程中。由于我国普及计算机、接入互联网的时间比国外晚,所以在网络安全方面的深入研究相对较晚。根据我国信息化发展的历史轨迹,总体可分为四个阶段。第一阶段,1999 年以前,初步接触网络,立法体现单一性、原则性。第二阶段,1999—2005 年,网络安全问题初现,立法开始关注新问题。第三阶段,2005—2012 年,一方面,网络使用普及化,对传统行业冲击巨大,网络极大地改变了社会生产方式,社会经济全面繁荣,我国成为网络大国;另一方面,国际社会动荡,网络安全形势严峻,立法体现多元化与积极性,战略性文件出台,引领信息化与网络安全保障工作。第四阶段,2012 年至今,国际层面竞争空前激烈,网络安全问题已成为全球共同面对的难题,网络安全战略性、全局性凸显,我国开始提出建设网络强国新目标,网络安全立法位阶提高,以《网络安全法》为标志,网络空间法治化体系现雏形。

## 第一节 1999 年以前

### 一、典型事件

1986 年 2 月,国务院批复成立国家经济信息中心,负责建设国家经济信息系



统。1988年去掉“经济”两字，更名为国家信息中心。该信息中心的发展为之后国务院信息化工作办公室的建立奠定了基础。

## 二、立法情况

1994年2月18日国务院令第147号《中华人民共和国计算机信息系统安全保护条例》发布。该条例是我国首部保护计算机信息系统安全的行政法规，开创了国际出入口信道专营制度；联网接入的许可、备案制度；计算机系统等级保护制度等基础制度，沿用至今。

1997年10月1日起实施的《刑法》首次规定了计算机相关犯罪，并纳入分则第六章妨害社会管理秩序罪第一节——扰乱公共秩序罪项下。具体而言，第285、286、287条分别设立了非法侵入计算机信息系统罪、破坏计算机信息系统罪，并对利用计算机实施犯罪进行了提示性规定。

## 三、本阶段立法特征

基于我国开始逐步接入国际互联网络，网络尚未被普遍使用的国情，本阶段立法主要规范网络接入活动，保障网络接入安全与计算机信息系统安全，尚未涉及实质的网络内容治理。部分规定呈现原则性、概括性，在之后的法律法规修订中对这些特征均有体现。

### 第二节 1999—2005年

#### 一、典型事件

1999年中国围剿千年虫，“千年虫”即“计算机2000年”问题。由于20世纪90年代人们生产生活中使用的很大一部分计算机或微机不支持四位数字的年份，即把2000年仍按照00年来计算，这引发了信息系统的计时紊乱，如果不能

及时处置，将造成计算机信息系统功能紊乱，从而引发经济、军事、科学计算与人类社会生活的一系列连锁反应。从1999年4月起，北京市相关部门组织专家对全市水、电、气、热等涉及国计民生的重点行业的重点单位进行了大检查，全国银行业停业测试。检查结果为关系国计民生的行业都有较好的准备与应急措施，2000年前后未发生重大问题。

2001年中美黑客大战。同年4月1日美军一架侦察机侵入中国领空，撞毁中国跟踪监视其严重侵犯中国主权行为的军用飞机，导致了一场大规模的中美黑客大战。五一期间，中国黑客反击战正式打响，全世界黑客分营助威中美黑客网络大战升温。这次中美网络大战，使两国不少网站损失惨重。大战中被攻破的美国网站约1600个，其中主要网站（包括美国政府和军方的网站）有900多个，中国被攻破的网站则有1100多个，重要网站多达600个。

2001年成立国务院信息化工作办公室。8月23日，中共中央、国务院决定重新组建国家信息化领导小组，以进一步加强对推进我国信息化建设和维护国家信息安全工作的领导。同年12月正式设立办事机构，即国务院信息化工作办公室。国家信息化领导小组负责审议国家信息化的发展战略，宏观规划，有关规章、草案和重大的决策，综合协调信息化和信息安全的工作。

## 二、立法情况

1999年10月7日国务院制定颁布《商用密码管理条例》<sup>①</sup>。该条例界定了商用密码的定义，强调商用密码技术属于国家秘密，国家对此实行专控管理。在明确规定加强商用密码管理的目的、范围、基本原则、罚则、主管及委托分管的组织机构的同时，对商用密码产品的科研、生产、销售、使用等具体环节的管理措施都做出了规定。

2000年9月国务院发布292号令《互联网信息服务管理办法》<sup>②</sup>，规范在中国境内进行的互联网信息服务行为。该办法对互联网信息服务提供者及其信息服务行为进行规范，用法规形式保障信息运行与内容安全，标志我国互联网监管进

---

① 参考 [http://www.oscca.gov.cn/News/200512/News\\_1053.htm](http://www.oscca.gov.cn/News/200512/News_1053.htm)。

② 参考 [http://www.gov.cn/fwxx/bw/gjgbdydszj/content\\_2263004.htm](http://www.gov.cn/fwxx/bw/gjgbdydszj/content_2263004.htm)。

入体系化阶段。

2000年9月25日公布实施的《电信条例》旨在规范电信市场秩序，维护电信用户和电信业务经营者的合法权益，保障电信网络和信息的安全，促进电信业的健康发展。该条例对电信市场、电信服务、电信建设等活动进行规范的同时，特立一章强调电信安全。

2000年12月28日全国人大常委会通过《关于维护互联网安全的决定》<sup>①</sup>，为保障国家安全、公共利益、个人合法权益，特强调危害互联网的运行安全、危害国家安全和社会稳定、社会主义市场经济秩序和社会管理秩序，危害个人、法人和其他组织的人身、财产等合法权利，构成刑事犯罪的应依法追究刑事责任，违反行政法规或民事法律的，依法承担相应责任。该决定通过清晰的指引起到有效的预防作用。与此同时，要求各级政府和有关部门加强监管，司法机关、执法机关各司其职，推进网络领域法治化建设。

2003年9月7日中共中央办公厅、国务院办公厅发出通知，转发《国家信息化领导小组关于加强信息安全保障工作的意见》<sup>②</sup>（中办发[2003]27号）结合我国信息化全面发展、信息安全面临挑战的国情，共提出十项意见，其中第七条强调加强信息安全法制建设和标准化建设。至此，将研究起草《网络安全法》提上日程。强调要建立和完善信息安全法律制度，明确社会各方面保障信息安全的责任和义务，积极参与国际信息网络规则的制定，开展涉及信息网络的国际司法协助。与此同时，重视信息安全执法队伍建设，加强对利用网络传播有害信息、危害公众利益和国家安全的违法犯罪活动的打击。

### 三、本阶段立法特征

随着对互联网的进一步接入和使用，网络的双面性开始显现：一方面，网络能够方便人们的生产、生活，优化传统行业的经营模式，进而使得人对网络的依赖性增强；另一方面，网络固有的缺陷属性显现，针对网络的攻击行为、网络信息内容传播行为均难以控制，安全、可控成为本阶段立法的目标。此时，除了专

<sup>①</sup> 参考 [http://www.npc.gov.cn/wxzl/gongbao/2001-03/05/content\\_5131101.htm](http://www.npc.gov.cn/wxzl/gongbao/2001-03/05/content_5131101.htm)。

<sup>②</sup> 参考 <http://www.waizi.org.cn/law/9235.html>。

门的《电信条例》强调电信安全，《互联网信息服务管理办法》首次强调内容安全以外，相关主管部门开始呼吁起草专门的基础性立法——《网络安全法》。

监管方面，首次完成体系建设工作，构建了包含网络层、接入层、业务层、内容层的监管框架。与此同时，以信息产业部、公安部及内容主管部门为代表的监管主体地位确立和明晰，但总体监管格局显现“齐抓共管、各负其责”的特征。

### 第三节 2005—2012 年

#### 一、典型事件

“熊猫烧香”病毒大肆传播。2006 年年底到 2007 年年初，国内名为“熊猫烧香”的病毒不断入侵个人计算机、感染门户网站、击溃数据系统，给百万个人用户、网吧及企业局域网用户带来了无法估量的损失。“熊猫烧香”传播性极高，中病毒者会在短时间内传染局域网内其他用户，之后通过变种持续危害网络安全，至 2016 年才逐渐消失。

2007 年 4 月，爱沙尼亚政府被黑。黑客目标包括国会、政府部门、银行，甚至媒体网站，其攻击规模广泛而且深入，被军事专家视为第一场国家层次的网络战争。爱沙尼亚是历史上第一个政府和关键基础设施经历大规模网络攻击的国家。该事件发生了 3 个星期，这标志着一种新的、难以追踪、影响国际安全、没有固定模式的威胁的开始。

2008 年 3 月撤销国信办。由于国家启动大部制改革，国务院信息化办公室被撤销。依据《国务院关于机构设置的通知》（国发〔2008〕11 号），办公室工作职责被纳入新成立的工业和信息化部。

2009 年 7 月 5 日，新疆乌鲁木齐发生打砸抢烧严重暴力犯罪活动。据报道，此前以民族分裂分子热比娅为首的“世界维吾尔代表大会”通过互联网等多种渠道煽动暴动活动。“7·5”事件是 1949 年以来在新疆历次事件中造成人员伤亡和经济财产损失最严重的一次。

2010年1月,谷歌退出中国。谷歌自称遭受网络攻击,于13日宣布考虑退出中国。然而在前一天,百度在美的域名注册商处被非法篡改。这两个事件折射出互联网公司走出去所面临的安全问题。

2010年9月27日,在腾讯发布产品QQ医生之后,360发布QQ保镖,两款安全产品之争引发一场持久大战。至2012年11月3日,腾讯强迫用户“二选一”将此事推向高潮。网络公司的竞争开始直接影响用户对网络产品的使用,此事件成为我国互联网公司市场竞争的典型案例。

2010年6月,“震网”病毒被首次检测出来。该病毒是第一个专门定向攻击真实世界中基础(能源)设施的蠕虫病毒,如核电站、水坝、国家电网等。据《中国解放军报》报道,美国曾利用“震网”蠕虫病毒攻击伊朗的铀浓缩设备,已经造成伊朗核电站推迟发电。截至2011年,该病毒感染了全球超过45 000个网络,60%的个人计算机。至2013年我国国内已有近500万名网民及多个行业的领军企业遭此病毒攻击。据分析称,席卷全球工业界的“震网”病毒可导致伊朗的核工业倒退十年。

2010年12月发生的突尼斯茉莉花革命,是以一名26岁青年自焚为导火索,导致发生突尼斯境内大规模街头示威游行及争取民主的活动。然而,美国《外交政策》杂志称,维基解密网站曝光的总统家族腐败电文是突尼斯这次革命的催化剂,并指出这或许称得上是世界上第一场“维基革命”。该事件进而导致时任总统的本·阿里政权倒台,成为阿拉伯国家中第一场因人民起义导致推翻现政权的革命。

2012年5月,“火焰”病毒在中东地区大范围传播,其中伊朗受病毒影响最严重。“火焰”病毒是一种破坏力巨大的全新计算机蠕虫病毒。据分析称,网络战早已不是一种概念,而是现实。与“震网”病毒相比,“火焰”病毒更为智能,攻击机制更为复杂,且攻击目标具有特定地域的特点。

## 二、立法情况

2006年国务院发布《国家中长期科学和技术发展规划纲要(2006—2020年)》对重点领域、优先主题进行定义,确定优先主题原则;重点安排8个技术领域的27项前沿技术,18个基础科学问题,并提出实施4个重大科学研究计划。信息产

业及现代服务业为 8 个技术领域之一。纲要指出发展信息产业和现代服务业是推进新型工业化的关键。

2006 年,《2006—2020 年国家信息化发展规划》结合全球信息化趋势与我国信息化建设的基本情况,指出我国信息化建设的战略重点。明确应全面加强建设国家信息安全保障体系。做到两个坚持:坚持积极防御、综合防范,探索和把握信息化与信息安全的内在规律,主动应对信息安全挑战,实现信息化与信息安全协调发展;坚持立足国情,综合平衡安全成本和风险,确保重点,优化信息安全资源配置。建立和完善信息安全等级保护制度,重点保护基础信息网络和关系国家安全、经济命脉、社会稳定的重要信息系统。加强密码技术的开发利用。建设网络信任体系。强调加强信息安全风险评估工作,建设完善信息安全监控体系,提高对网络安全事件的应对和防范能力,防止有害信息传播。要求高度重视信息安全应急处置工作,健全完善信息安全应急指挥和安全通报制度,不断完善信息安全应急处置预案,促进资源共享,重视灾难备份建设,增强信息基础设施和重要信息系统的抗毁能力和灾难恢复能力。

2007 年 6 月 22 日公安部、国家保密局、国家密码管理局、国务院信息化工作办公室联合发布印发《信息安全等级保护管理办法》的通知。该办法为《计算机信息系统安全保护条例》中所规定的关于安全等级划分标准和安全等级保护的具体办法。该办法强调国家信息安全等级保护坚持自主定级、自主保护的原则,将信息系统的安全保护等级分为五级。不同等级受到不同程度的建设、运营、监管。该办法对涉及国家秘密的系统分级保护进行专门规定,并对信息安全等级保护的密码分级管理进行规定。

2009 年 2 月 28 日全国人大常委会通过《刑法修正案(七)》<sup>①</sup>扩大《刑法》所保护的法益。在《刑法》第二百五十三条后增加侵犯公民个人信息罪,犯罪主体为国家机关或金融、电信、交通、教育、医疗等单位的工作人员,并规定了单位犯罪。在《刑法》第二百八十五条中增加侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统以外的计算机信息系统及其中数据作为保护对象。首次将制作入侵程序、工具,对明知他人违法行为提供程序、工具帮助作为犯罪行

---

<sup>①</sup> 参考 [http://www.npc.gov.cn/npc/xinwen/lfgz/zxfl/2009-02/28/content\\_1476574.htm](http://www.npc.gov.cn/npc/xinwen/lfgz/zxfl/2009-02/28/content_1476574.htm)。

为构成要件进行规定。至此，将有效打击非法侵入计算机信息系统、非法侵害公民个人信息的犯罪行为。

2010年10月1日起施行的《保守国家秘密法》有显著修改之处，如对国家秘密的范围进行了缩小，明确保密与公开的关系，保密工作既要确保国家秘密安全，又要便利信息资源合理利用；增加了确定国家秘密事项的标准，增加了定密责任人制度，增加了定密层级和定密权限的规定，增加了保密期限与及时解密条件的规定。

2012年6月，国务院发布《关于大力推进信息化和加强信息安全保障的若干意见》强调大力推进信息化发展和切实保障信息安全，对调整经济结构、转变发展方式、保障和改善民生、维护国家安全具有重大意义。结合当前严峻的国际竞争与安全问题，指出我国信息化建设还面临很多劣势。例如，宽带信息基础设施发展水平与发达国家的差距有所拉大，政务信息共享和业务协同水平不高，核心技术受制于人，信息安全工作的战略统筹和综合协调不够，重要信息系统和基础信息网络安全防护能力不强，移动互联网等技术应用给信息安全带来严峻挑战。特别提出加强信息安全保障工作的几点意见。在加快“宽带中国”工程实施、促进信息化的同时，特别强调健全安全防护和管理，保障重点领域信息安全。确保重要信息系统和基础信息网络安全，加强政府和涉密信息系统安全管理，保障工业控制系统安全，强化信息资源和个人信息保护。

### 三、本阶段立法特征

本阶段，我国网络使用率大幅提高，网络产业迅速发展，网络服务新形态不断涌现，国内外网络安全事件频发，影响较为深入、广泛。网络安全相关立法呈现多元化、战略性与操作性相结合的特征。多元化体现在强调保守国家秘密的同时，开始规范互联网竞争行为，指导互联网行业发展。战略性体现在发布多部纲要，推进信息化建设与信息安全保障工作。

监管方面，伴随2008年的大部制改革，国务院信息化办公室被撤销，国家信息化领导体制有所弱化，与此对应，互联网监管部门的主体地位得到提升。至此，网络领域多头监管的弊端开始显现。

## 第四节 2012 年至今

### 一、典型事件

华为海外收购受阻。早在 2008 年，华为试图收购美国电信企业 3COM 公司，因美国政府对国家安全的担忧而放弃。2010 年，华为再次收购 3COM 公司和摩托罗拉网络设备部门仍受阻。2011 年 11 月，美国众议院情报委员会调查华为、中兴等中国企业在美扩张业务过程中是否会给美国国家安全带来潜在威胁。2012 年 8 月，美国国际贸易委员会宣布对来自中国等多个国家和地区的企业生产的无线电子设备发起大规模的“337 调查”，以确定这些企业是否侵犯美国企业的专利，华为、中兴、宏达等知名企业均为被调查对象。前述情况，反映出中国通信设备企业走出去面临的国际环境。

2013 年 6 月发生斯诺登事件。斯诺登将美国国家安全局关于“棱镜计划”监听项目的秘密文档披露给了《卫报》和《华盛顿邮报》，通过该计划，美国国家安全局可以接触到大量个人聊天日志、存储的数据、语音通信、文件传输、个人社交网络数据，这是一起美国有史以来最大的监控事件。

2014 年索尼影业被黑。11 月 12 日黑客组织“和平卫士”公布索尼影业员工电邮，涉及公司高管薪酬和索尼非发行电影拷贝等内容。同年 12 月 15 日，两名前索尼影业员工以索尼影业不保护他们被黑客泄露的数据为由，将索尼公司诉至法院。

2015 年中国军人被起诉。2015 年 7 月 28 日美国司法部起诉前中国军人陈伟，称其于 2013 年在科威特担任美国国防部外包人员期间，损坏美国军方计算机，复制美方机密文件，并隐瞒背景来通过机密级别安全审查。

2015 年《瓦森纳协定》修改。该协定全称为《关于常规武器和两用物品及技术出口控制的瓦森纳安排》。2015 年 5 月，美国商务部工业与安全局公布《瓦森纳协定》的修改草案。2016 年 12 月在维也纳召开的《瓦森纳协定》会议上，美国试图再次修订《瓦森纳协定》。此次修订后网络安全工具出口将更容易，但该修



订最终未获通过。

2015 年中美网络安全谈判。2015 年 9 月美国和中国讨论了首个网络空间军备控制协议，双方共同承诺在和平时期不首先使用网络武器破坏另一方的关键基础设施。据分析，该协议可能成为国际网络空间行为准则的范本。中美谈判，就打击网络间谍等网络安全问题达成共识，拟构建新型大国关系。

2015 年 12 月，乌克兰电网遭受攻击。黑客攻击乌克兰电网的控制系统，造成其首都基辅附近断电超一小时，数百万户家庭被迫供电中断。这是有史以来首次导致停电的网络攻击。

2016 年中兴供应链事件。2016 年 3 月 7 日，美国商务部认为中兴违规向伊朗销售禁运产品，旋即对中兴发出限制采购零部件令。此次禁令虽于 3 月 24 日暂时解除，但暴露出中兴等中国电信设备企业在供应链上对外的依赖，在高端原材料生产科学技术方面相对落后。

2016 年 7 月，土耳其政变。土耳其时间 2016 年 7 月 15 日，土耳其武装部队总参谋部部分军官企图发动军事政变，部分军人通过控制土耳其广播电视协会电视台宣布军队已接管政权。政变期间多人伤亡、汇率波动、机场停飞，社交媒体一度瘫痪，如“推特”、“脸书”和“YouTube”等不能连接至互联网，用户无法正常使用社交网络。

2017 年“想哭”蠕虫病毒爆发。5 月 12 日，一款直译名为“想哭”(WannaCry)的蠕虫式勒索病毒在英国爆发，并在全球范围迅速蔓延。近一周时间有 100 多个国家的数十万名用户中招，政府、医疗、教育、能源、通信、金融等多个重点领域受到影响。此次事件对我国也造成了一定程度的影响。

## 二、立法情况

2012 年 12 月 28 日全国人大常委会发布《关于加强网络信息保护的决定》<sup>①</sup>以决定的形式从维护信息内容安全、保障个人信息安全、落实实名制等角度加强网络信息保护。

---

<sup>①</sup> 参考 [http://www.gov.cn/jrzq/2012-12/28/content\\_2301231.htm](http://www.gov.cn/jrzq/2012-12/28/content_2301231.htm)。

2013 年 11 月 9 日十八届四中全会《中共中央关于全面深化改革若干重大问题的决定》中强调,“加大依法管理网络力度,加快完善互联网管理领导体制,确保国家网络和信息安全”。

2014 年 2 月 27 日,我国成立了“中央网络安全和信息化领导小组”,习近平总书记发表重要讲话指出,“网络安全和信息化是事关国家安全和国家发展、事关广大人民群众工作生活的重大战略问题”。

2014 年 3 月实施《中华人民共和国保守国家秘密法实施条例》<sup>①</sup>。该条例适贯彻实施保密法及社会经济发展的需要,对《保密法》的制度进行了细化,促进落地。例如,条例规范了国家秘密保护与信息公开的关系,对保密事项范围基本内容和形式做出统一规定,体现了保密事项范围的规范性要求,为机关、单位准确定密提供了可直接对照的依据,大大提高了《保密法》的操作性。

2014 年 10 月 23 日十八届四中全会《中共中央关于全面推进依法治国若干重大问题的决定》强调贯彻落实总体国家安全观,加快建设社会主义法治国家,建设中国特色社会主义法治体系,强调加强互联网领域立法,完善网络信息服务、网络安全保护、网络社会管理等方面的法律法规,依法规范网络行为,推进社会治安综合治理,依法强化破坏网络安全等重点问题的治理。

2015 年中俄签订网络安全协定,全称《中华人民共和国政府和俄罗斯联邦政府关于在保障国际信息安全领域合作协定》。协定规划两国合作的主要方向,如建立共同应对国际信息安全威胁的交流沟通机制,在打击恐怖主义和犯罪活动、人才、科研、应急响应等领域展开合作。

2015 年 7 月 1 日通过《国家安全法》<sup>②</sup>,以法律的形式确立了总体国家安全观的指导地位和国家安全领导体制。特别规定国家安全保障内容,强调国家健全国家安全法律制度体系,推动国家安全法治建设。

2015 年 11 月,《刑法(修正案九)》加强公民个人信息保护,去掉相关犯罪主体的限制,即删掉履行职务的国家机关、金融、电信等单位工作人员的规定,强调履行职务过程中或提供服务过程中获取的公民个人信息,不得出售或提供他人,并且同样将此条规定为单位犯罪。严惩恐怖主义、极端主义犯罪活动,维

① 参考 [http://www.gov.cn/jwqk/2014-02/03/content\\_2579949.htm](http://www.gov.cn/jwqk/2014-02/03/content_2579949.htm)。

② 参考 [http://www.npc.gov.cn/npc/xinwen/2015-07/07/content\\_1941161.htm](http://www.npc.gov.cn/npc/xinwen/2015-07/07/content_1941161.htm)。

护网络信息安全，新增编造虚假信息罪。加强非法侵入计算机信息系统罪、破坏计算机信息系统罪的处罚力度。例如，增加第二百八十五条、第二百八十六条、第二百八十七条对单位犯罪的规定。与此同时，增加网络安全服务提供者违法安全管理义务罪。故意帮助网络违法犯罪活动的，同样构罪。

2015年12月27日全国人大常委会通过《反恐怖主义法》<sup>①</sup>，作为一项基本法对恐怖活动组织和人员的认定、安全防范、情报信息、调查、应对处置、国际合作、保障措施、法律责任等方面进行了规定。特别强调各监管部门的职责及电信业务经营者、互联网服务提供者的屏蔽与报告义务。

2016年3月17日《十三五规划纲要》<sup>②</sup>明确指出要拓展网络经济空间，把握信息技术变革趋势，实施网络强国战略，加快建设数字中国，推动信息技术与经济社会发展深度融合，加快推动信息经济发展壮大。构建泛在高效的信息网络，发展现代互联网产业体系，实施国家大数据战略，强化信息安全保障。

2016年习近平总书记“4·19”讲话，继续明确了国家安全与网络安全的关系，指出网络安全和信息化是相辅相成的。安全是发展的前提，发展是安全的保障，安全和发展要同步推进。讲话特别指出国家关键信息基础设施面临较大风险隐患，网络安全防控能力薄弱，难以有效应对国家级、有组织的高强度网络攻击。

2016年7月，中共中央办公厅、国务院办公厅印发《国家信息化发展战略纲要》<sup>③</sup>，并发出通知，要求各地区各部门结合实际认真贯彻落实。该纲要是根据新形势对《2006—2020年国家信息化发展战略》的调整和发展。基于国家信息化基本形势、指导思想、战略目标和基本方针，提出战略核心要点如大力增强信息化发展能力，着力提升经济社会信息化水平。强调不断优化信息化发展环境，推进信息化法治建设，加强网络生态治理，维护网络空间安全并重视体制保障和制度实施。

2016年11月16日习近平总书记在第三届世界互联网大会讲话，指出互联网发展是无国界、无边界的，利用好、发展好、治理好互联网必须深化网络空间国际合作，携手构建网络空间命运共同体。在强调坚持网络主权理念的前提下，中

① 参考 [http://www.npc.gov.cn/npc/xinwen/2015-12/28/content\\_1957401.htm](http://www.npc.gov.cn/npc/xinwen/2015-12/28/content_1957401.htm)。

② 参考 [http://news.ifeng.com/a/20160317/47926128\\_1.shtml](http://news.ifeng.com/a/20160317/47926128_1.shtml)。

③ 参考 [http://www.gov.cn/gongbao/content/2016/content\\_5100032.htm](http://www.gov.cn/gongbao/content/2016/content_5100032.htm)。

国愿与国际社会一道推动全球互联网治理，推动网络空间实现平等尊重、创新发展、开放共享、安全有序的目标。

2016年12月27日国家互联网信息办公室发布《国家网络空间安全战略》作为建设网络强国的动员令，强调完善网络治理体系，依法治理网络空间，健全网络安全法律法规体系，制定出台《网络安全法》、《未成年人保护条例》等法律法规。加快对现行法律的修订和解释以适用于网络空间。促进行政监管法治化水平，鼓励公众参与网络治理。

2017年6月《网络安全法》作为我国第一部网络空间综合性法律，有效地弥补了我国网络安全法律领域的空缺，在我国网络空间立法进程中具有里程碑式的意义，同时也是依法治国基本方略的重要体现。该法特别重视贯彻落实总体国家安全观的法制理念。在应对网络空间治理问题中，既重视传统安全，又重视非传统安全；既重视发展问题，又重视安全问题；既重视自身问题，又重视共同安全。在具体规定上既重视网络入侵，又重视网络攻击；既重视网络风险，又重视网络威胁；既重视基础性安全，又重视应急处置；既重视网络运营商法规遵从，又重视违法犯罪的打击惩治。中国以实际行动提升网络空间治理水平，彰显一个负责任大国的形象。

### 三、本阶段立法特征

《网络安全法》是我国首部网络安全领域基本法律，在我国网络安全立法历史上具有里程碑的意义，网络安全法治体系建设显现初步成果。立法层级升高，多部安全方面的立法出台。网络安全战略性、全局性凸显，引战略入法。法律规范紧跟产业发展，监管深入细致，权责更加清晰，法规可操作性增强。

以上四个阶段的网络安全事件及相关立法发展情况充分体现了我国立法与时俱进、不断完善的整体特征。网络空间面临的威胁类型呈现由技术简单、目的单一到技术难度提高、多层面、复合化的发展趋势，因此以此为基础的网络威胁治理模式也需要与时俱进、不断完善。未来网络空间治理，一方面需要基于本国国情不断创新、夯实技术与经济基础；另一方面需要走出去，加强国际合作与交流，借鉴优秀经验，共同抵御网络安全威胁；防治结合，共建国际层面多边、民主、透明的互联网治理体系。

# 《网络安全法》的基本原理

## 第一节 《网络安全法》的制定背景

### 一、时代背景

当前我国面临的国内和国际信息安全形势相当复杂和严峻，境外敌对势力的网络浸透日益泛化，国内各种极端势力进行的网络恐怖活动及社会矛盾交融所产生的国家和社会稳定任务更加迫切。“多网域跨际”和“供应链渗透”威胁着能源、通信、金融、工业等国家关键基础设施安全。大数据挖掘和数据跨境流动广泛融入现代商业的发展模式中，给涉及我国商业运行数据、公民个人敏感数据等国家数据主权，特别是国家独立的司法权力架构带来了结构性的挑战。同时，我国企业走出国门的“拐点”已经来临，国家经济发展“走出去”与“引进来”的发展战略需要进行重大调整。

世界层面，和平与发展仍为时代主题，随着世界多极化、经济全球化、文化多样化、社会信息化深入发展，国家间竞争空前激烈，传统安全与非传统安全交织，国际关系复杂程度前所未有。网络空间已成为各国竞争与博弈的新疆域，网络安全的战略性、全局性凸显。网络安全问题成为全球共同面对的问题，斯诺登事件、乌克兰电网遭遇攻击，“想哭”蠕虫病毒全球扩散，反映网络空间并非孤岛，国家间合作亟待加强。2016 年第三届世界互联网大会就以“创新驱动

动造福人类——携手共建网络空间命运共同体”为主题。

面对当前国内、国际网络安全战略性、全局性凸显的新形势，国家迫切需要一部综合性的统领信息化发展的立法。2014年2月27日，我国成立了“中央网络安全和信息化领导小组”，习近平总书记发表重要讲话指出，“网络安全和信息化是事关国家安全和国家发展、事关广大人民群众工作生活的重大战略问题”。习近平总书记在2016年“4·19”重要讲话中继续明确了国家安全与网络安全的关系，指出当前网络安全威胁和风险日益突出，并日益向政治、经济、文化、社会、生态、国防等领域传导渗透；强调目前我国针对国家关键信息基础设施的网络安全防护能力较为薄弱。

同年，《十三五规划纲要》<sup>①</sup>明确要求拓展网络经济空间，重点实施网络强国治理战略，强化信息安全保障。随后，国家互联网信息办公室发布《国家网络空间安全战略》。强调完善网络治理体系，依法治理网络空间，健全网络安全法律法规体系，加快制定出台《网络安全法》。2017年6月1日，作为我国第一部网络空间综合性法律的《网络安全法》正式生效，该法特别重视贯彻落实总体国家安全观的法制理念，在我国网络空间立法进程中具有里程碑式的意义，同时也是依法治国基本方略的重要体现。

## 二、技术背景

当今时代，又被称为大数据时代，大数据意味着数据体量巨大、种类繁多。网络空间的海量数据不仅关系个人隐私、社会经济发展状况，更关系国计民生与国家安全。一方面，大数据是国家的重要资源，是互联网产业发展壮大的重要支撑。十三五规划着眼对数字经济价值的发挥，强调把大数据作为基础性战略资源，全面实施促进大数据发展行动，加快推动数据资源共享开放和开发应用，助力产业转型升级和社会治理创新。另一方面，大数据的又一价值即威胁情报分析。换言之，数据本身既是网络安全保护的对象，又是可用于进行网络安全保护的重要信息来源和技术工具。

云计算技术的发展，改变以往数据的存储方式，使得数据流动变得自动化或

---

<sup>①</sup> 参考 [http://news.ifeng.com/a/20160317/47926128\\_1.shtml](http://news.ifeng.com/a/20160317/47926128_1.shtml)。

难以控制监管，尤其是跨境数据流动成本更加便宜。云安全是数据安全的保证，与此同时，云计算促进数据跨境流动常态化，引发人们对数据主权问题的思考。

### 三、国际背景

网络安全问题无国界，国家间竞争激烈、矛盾冲突的同时有合作的可能性。

#### （一）网络安全事件影响广泛深刻

网络技术日新月异，促进社会经济繁荣发展的同时，人们对网络“恶”的利用也尽显网络之恶，网络的“双刃剑”性质体现突出。当前的网络攻击事件已经远非黑客个人炫耀技能之目的，攻击的目标性更强，已经严重损害关键信息基础设施安全，因网络而起的恐怖暴动事件甚至危及政府统治。以乌克兰电网遭遇攻击为例，国家关键信息基础设施已成为攻击目标。突尼斯茉莉花革命甚至颠覆了国家政权。最近的“想哭”蠕虫病毒，通过改造被公开的美国国家安全局武器库的“永恒之蓝”，利用 Windows 系统漏洞发起攻击。其影响范围广泛、深刻。近一周时间，100 多个国家的数十万名用户中招，医疗、教育、能源、通信、金融等行业受到波及，给全球网络安全保护工作提出了值得重视的问题。

#### （二）国家间合作交流深化

随着贸易全球化，跨国公司不断发展壮大，国家间经济合作交流频繁。在网络安全方面，各国开始寻求合作，共同治理。

2010 年 7 月，包括美国、俄罗斯和中国在内的 15 个国家向联合国秘书长递交一系列磋商建议，呼吁各国开展更为有效的合作，这是首次世界主要国家在网络安全问题上达成共识。

2013 年 6 月，奥巴马与普京联合宣布，美俄已经达成了在网络领域建立信任措施的首份双边协议，内容包括信息交换和危机沟通等。

2015 年美国和中国讨论了首个网络空间军备控制协议，双方共同承诺在和平时期不首先使用网络武器破坏另一方的关键基础设施。双方就打击网络间谍等网络安全问题达成共识，双方愿意构建新型大国关系。

2016 年德国联邦情报局与美国国家安全局恢复了网络监控合作。同年 2 月 11 日，北约和欧盟达成一项技术协议以加强网络安全合作，共同应对日益严峻的网络威胁。5 月 5 日，韩国与美国就共同开发技术、进一步分享全球网络威胁信息、加强网络安全政策对接、携手打击网络恐怖主义等达成合作共识。

### （三）各国的网络安全战略与立法

为应对层出不穷的网络安全威胁，各国纷纷加大了网络安全治理与立法的力度。网络安全战略紧跟当前国际、国内网络安全形态，规划符合新形势的网络安全战略目标。立法层面，以战略为指导，综合立法与专门立法相结合，着眼具体制度、问题对维护网络安全进行明确指引，以几个典型国家为例。

#### 1. 战略方面

美国政府较早关注网络空间固有特征对关键信息基础设施的威胁，并逐步发布战略性文件。美国主要的战略性文件包括《网络空间安全国家战略》、《网络空间国际战略》和《网络空间行动战略》。2016 年年底，美国战略与国际研究中心发布《从认知到行动——第四十五任美国总统安全议程》报告，为特朗普政府提供未来五年网络安全战略建议，其中包括国际战略、打击网络犯罪、保护全球数据安全、“基准”网络安全、关键性基础设施 NIST 框架，数据保护、隐私与网络安全，提高网络事件透明度，保障物联网安全、支持强加密策略，减少安全漏洞，提升功效与云服务的利用率，加强人才建设等。

2011 年英国政府发布了《国家网络安全战略》，报告提出将在 2016—2021 年投资约 19 亿英镑用于加强网络安全能力。该战略包含三大要点：防御、威慑和发展。

2013 年 7 月欧盟委员会颁布《欧盟网络安全战略：公开、可靠和安全的网络空间》。该战略是欧盟在网络安全领域的首个政策性文件，强调提升网络的抗打击能力、大幅减少网络犯罪、在欧盟共同防务的框架下制定网络防御政策和发展防御能力、发展网络安全方面的工业和技术、为欧盟制定国际网络空间政策。

#### 2. 立法方面

美国截至 2017 年颁布了超过 50 部法案来规范网络安全领域相关活动。2010



年美国延长了《爱国者法案》的效力。美国“9·11事件”以后，网络与信息安全在美国引起了更强烈的重视。美国政府以保障国土安全和反恐为名颁布了《爱国者法案》，按照该法案，有关部门可对公民进行窃听，查看公民上网记录、私人信件和电子邮件，甚至允许联邦调查局监视公民阅读书籍的情况，从图书馆收集读者的读书记录，从而判断读者是否受到恐怖主义影响。《外国情报监听法》同《爱国者法案》一道被作为实施信息监听的法律依据。2012年，美国将《联邦信息安全管理法》更新为《联邦信息安全改革法》，强调对计算机网络进行实时、自动监控，加强联邦政府网络安全保护。2014年通过了《国家网络安全保护法》，强化了国土安全部的国家网络安全和通信集成中心在联邦部门和私有部门共享网络安全信息方面的重要作用，为立足国家层面部署和加强公共和私有部门网络安全信息共享提供法律依据。2015年美国通过了将《网络安全法》作为《2016年综合拨款法案》中的一部分，网络安全信息共享为其核心内容。

2016年7月欧盟通过了《网络与信息安全指令》，欧盟层面的首部网络安全法案正式出台。在宏观层面，要求欧盟各国应制定自身的网络与信息安全国家战略，加强网络安全方面的合作交流。在微观层面，强调加强基础服务运营者、数字服务提供者的网络与信息系统之安全，要求这两者履行网络风险管理、网络安全事故应对与通知等义务。同年，欧盟修订《通用数据保护规则》，加强对数据安全保护。

我国《网络安全法》的出台，是我国依法治国、依法治网的重要法律依据，成为我国网络空间法治建设里程碑式的标志，是对“总体国家安全观”及“安全与发展一体两翼”的国家战略在国家法律层面做出的积极应对。

## 第二节 《网络安全法》与相关立法的关系

### 一、《网络安全法》的本质特征

《网络安全法》是我国网络空间法治建设的重要里程碑，是我国第一部关于网络安全的基础性法律。《网络安全法》具有“保障法”的属性，即保障网络运行安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织

的合法权益，促进经济社会信息化健康发展。重点保护关键信息基础设施运行安全，保障网络信息安全，重视网络安全风险的监测预警与网络安全事件应急处置。

《网络安全法》以社会公共利益为本位，具有“社会法”的属性。任何法的目的都有其存在的社会经济基础，《网络安全法》也不例外。随着信息系统的网络化发展，网络成为国民经济和社会发展的先进生产力。网络安全保障法就具有明显的“社会法”属性，社会公共利益成为发展信息网络、保障经济和社会发展的根本利益。我们必须清醒地认识到，在以信息化带动工业化、全面推动国民经济和社会发展的过程中，社会公共利益与个体利益的冲突是主要的、不可避免的，此时的社会公共利益可适当优先于个体利益。

## 二、与相关立法的关系

### （一）《网络安全法》与相关行政法规

#### 1. 《网络安全法》与《国家安全法》

国家安全体系集政治安全、国土安全、军事安全、经济安全、文化安全、社会安全、科技安全、信息安全、生态安全、资源安全、核安全等于一体。《国家安全法》涵盖了国家安全各领域的内容，很多都是原则性规定，重点解决国家安全各领域带有普遍性的问题和亟待立法填补空白的问题，同时为今后制定相关配套法律法规预留了空间。网络安全是国家安全的重要内容，其对国家安全和社会稳定产生的巨大影响日益凸显。尤其是新时期，网络安全的战略性、全局性特征明显，没有网络安全就没有国家安全，信息安全也是国家安全的重要部分。可以说《网络安全法》与《国家安全法》相互呼应，在推动我国网络安全建设和捍卫国家安全方面起到重要的推动作用。

从宏观上来看，《网络安全法》的立法宗旨是“保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展”。《国家安全法》的立法宗旨在于“维护国家安全，保卫人民民主专政的政权和中国特色社会主义制度，保护人民的根本利益，保障改革开放和社会主义现代化建设的顺利进行，实现中华民族伟大复兴”。在维护国家

安全,保护人民根本利益,保障社会稳定方面,两法的立法宗旨具有一致性。其中《国家安全法》第二十五条明确规定“国家建设网络与信息安全保障体系,提升网络与信息安全保护能力,加强网络和信息技术的创新研究和开发应用,实现网络和信息核心技术、关键基础设施和重要领域信息系统及数据的安全可控;加强网络管理,防范、制止和依法惩治网络攻击、网络入侵、网络窃密、散布违法有害信息等网络违法犯罪行为,维护国家网络空间主权、安全和发展利益”。提出加强网络和信息安全保障,加强网络和信息技术创新开发,加强网络管理的要求,以立法形式将网络与信息安全提升到国家安全层面。

从具体制度设计上来看,《国家安全法》规定了监测预警制度,其第五十七条规定“国家健全国家安全风险监测预警制度,根据国家安全风险程度,及时发布相应风险预警”。《网络安全法》在第五章专门设置章节规定监测预警与应急处置,增强《国家安全法》的可操作性;《国家安全法》第五十九条对涉及国家安全事项的网络与信息安全保障做出了原则性的规定,“国家建立国家安全审查和监管的制度和机制,对影响或可能影响国家安全的外商投资、特定物项和关键技术、网络信息技术产品和服务、涉及国家安全事项的建设项目,以及其他重大事项和活动,进行国家安全审查,有效预防和化解国家安全风险”。而《网络安全法》作为网络安全监管领域的基础性法律,在《国家安全法》的原则指导性指导下,具体规定了实施细则,充分体现了两部法律在维护网络安全相关规定上的有效衔接。

网络安全保障的内容如果涉及国家安全,基于维护国家网络空间主权、安全和发展利益,将受到《国家安全法》的规制和保护。在此方面,《国家安全法》对涉及国家安全事项的网络与信息安全保障做出了原则性的规定;而《网络安全法》作为网络空间安全管理的基础性法律,在具体指导相关制度规定的有效实施方面起到重要作用,充分体现了两部法律在相关规定上的衔接。

## 2.《网络安全法》与《反恐怖主义法》

《网络安全法》与《反恐怖主义法》均是维护总体国家安全观的落地法律。在总体国家安全观的指导下,信息安全是国家安全的重要组成部分。《反恐怖主义法》针对网络恐怖主义犯罪规定了相关条款,在这方面体现了维护网络空间安全稳定运行的立法目的,与《网络安全法》在立法背景和立法原则方面相互呼应;《网络

安全法》关于协助调查、应急处置、安全审查等的制度设计对应《反恐怖主义法》的相关规定，为其提供具体的技术支持，加强其可操作性，在打击网络恐怖主义犯罪和维护网络空间安全运行方面，两法共同承担重要的责任。从宏观上来看，两者的总则规定具有重叠，《反恐怖主义法》在第二条中明确规定了“国家反对一切形式的恐怖主义”，其中包括网络恐怖主义。

在具体的制度设计中，《反恐怖主义法》在身份认证、对重点部位（行业、领域、目标）做重点防控、协助义务、应急处置方面都做出了具体规定。例如，《反恐怖主义法》第二十一条规定：电信、互联网、金融、住宿、长途客运、机动车租赁等业务经营者、服务提供者，应当对客户身份进行查验。对身份不明或拒绝身份查验的，不得提供服务……《反恐怖主义法》第二十七条第二款规定：地方各级人民政府应当根据需要，组织、督促有关建设单位在主要道路、交通枢纽、城市公共区域的重点部位，配备、安装公共安全视频图像信息系统等防范恐怖袭击的技防、物防设备、设施。第三十一条至三十四条分别对重点目标的管理、涉外、背景审查等做出了规定。这些规定在《网络安全法》中均有对应内容，《网络安全法》第二十四条明确规定，网络运营者为用户办理网络接入、域名注册服务，办理固定电话、移动电话等入网手续，或者为用户提供信息发布、即时通信等服务，在与用户签订协议或确认提供服务时，应当要求用户提供真实身份信息。用户不提供真实身份信息的，网络运营者不得为其提供相关服务。国家实施网络可信身份战略，支持研究开发安全、方便的电子身份认证技术，推动不同电子身份认证之间的互认；并在第二章第二节专门规定了保障关键技术设施的运行安全。

此外，《网络安全法》第三十四条、第三十五条明确规定，设置专门安全管理机构和安全负责人，并对该负责人和关键岗位的人员进行安全背景审查。关键信息基础设施的运营者采购网络产品和服务，可能影响国家安全的，应当通过国家网信部门会同国务院有关部门组织的国家安全审查。

可以说《网络安全法》做出了进一步细化，在打击恐怖主义涉网行为中，可实施性增强，更具有操作性，有利于网络安全保障措施和应对方案的有效实施。

### 3. 《网络安全法》与《治安管理处罚法》

《治安管理处罚法》作为维护社会治安秩序，保障公共安全，保护公民、法人和其他组织的合法权益，规范和保障公安机关及其人民警察依法履行治安管理职

责的基本法律，素有“小刑法”的称谓，与《刑法》的体系编排和内容设置均有交叉重叠。《治安管理处罚法》与《刑法》出于共同的价值目标即维护良好的社会秩序，在维护网络信息安全内容部分，《治安管理处罚法》第二十九条明确规定，利用计算机进行违法活动的，处五日以下拘留；情节较重的，处五日以上十日以下拘留：①违反国家规定，侵入计算机信息系统，造成危害的；②违反国家规定，对计算机信息系统功能进行删除、修改、增加、干扰，造成计算机信息系统不能正常运行的；③违反国家规定，对计算机信息系统中存储、处理、传输的数据和应用程序进行删除、修改、增加的；④故意制作、传播计算机病毒等破坏性程序，影响计算机信息系统正常运行的。与《刑法》相关内容呼应，在处罚范围方面有所区别：社会危害性小，尚不构成刑罚处罚范围的，应该适用《治安管理处罚法》的规定。

与《网络安全法》相比，在网络信息管理安全维护方面，《治安管理处罚法》的内容设置与《刑法》具有一致性，两法与《网络安全法》的区别也具有相似性。《治安管理处罚法》对危害网络安全的违法行为是事后的救济，而《网络安全法》构建了事前预防、事中监控、事后处罚“三位一体”的治理体系，从源头对网络攻击进行防范，在攻击发生时确保能够迅速响应与处置，将损害降至最低。在具体制度层面，《网络安全法》及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险；在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告；此外还明确要求国家也要建立网络安全监测预警和信息通报制度，范围比《治安管理处罚法》更加全面具体。可以说，在网络安全运行管理层面，打击危害网络安全管理制度的违法行为过程中，《网络安全法》更具有专业性和针对性，在《治安管理处罚法》未做出明确规定的情况下，应适用《网络安全法》。

#### 4. 《网络安全法》与《保密法》

《网络安全法》与《保密法》在法律位阶上属于同位阶法，都由全国人大常委会制定。《网络安全法》与《保密法》都从维护网络安全的根本目的出发，其中《网络安全法》第二十八条明确规定，网络运营者应当为公安机关、国家安全机关依法维护国家安全和侦查犯罪的活动提供技术支持和协助。《保密法》第九条规定，

下列涉及国家安全和利益的事项，泄露后可能损害国家在政治、经济、国防、外交等领域的安全和利益的，应当确定为国家秘密：维护国家安全活动和追查刑事犯罪中的秘密事项。因此，根据《网络安全法》第二十八条规定，网络运营者在为侦查机关提供必要的支持与协助过程中知悉或接触涉及国家秘密的事项，应当受《保密法》的规制与调整，有关人员不得泄露相关信息，否则将适用《保密法》追究其法律责任。

在具体制度方面，涉及国家秘密的网络安全管理事项受《保密法》作为特别法进行规制，如网络安全运行保障、信息系统存储处理的信息保护、信息处置和法律责任等方面的规定。例如，《保密法》第二十三条对网络安全等级保护制度做出了规定：存储、处理国家秘密的计算机信息系统（以下简称“涉密信息系统”）按照涉密程度实行分级保护。涉密信息系统应当按照国家保密标准配备保密设施、设备。保密设施、设备应当与涉密信息系统同步规划、同步建设、同步运行。涉密信息系统应当按照规定，经检查合格后，方可投入使用。本条确立了涉密信息系统的分级保护制度，并对其设备设施适用三同步原则。

《网络安全法》第二十一条，在保障网络运行安全方面，将网络安全等级保护制度上升至法律层面进行规制，要求网络运营者按照网络安全等级保护制度的要求，采取相应的管理措施和技术防范等措施，履行相应的网络安全保护义务。为了保障关键信息基础设施安全，维护国家安全、经济安全和保障民生，《网络安全法》进一步设专节对关键信息基础设施的运行安全做了规定，实行重点保护，并在第三十一条明确规定，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。由此可见，按照我国网络安全等级保护制度的相关规定，三级以上的信息系统即为涉密信息系统。在此方面，应当受到《保密法》的规制和保护，针对《保密法》中未做出规定的内容，应当适用《网络安全法》的相关规定，并且实行比其他信息系统保护更为严格的规定。在此方面，《保密法》可被视为《网络安全法》的特别法，在涉及涉密信息系统保护时优先予以适用。

《保密法》第二十四条规定了禁止实施的危害行为，机关、单位应当加强对涉密信息系统的管理，任何组织和个人不得有下列行为：①将涉密计算机、涉密存储设备接入互联网及其他公共信息网络；②在未采取防护措施的情况下，在涉密

信息系统与互联网及其他公共信息网络之间进行信息交换；③使用非涉密计算机、非涉密存储设备存储、处理国家秘密信息；④擅自卸载、修改涉密信息系统的安全技术程序、管理程序；⑤将未经安全技术处理的退出使用的涉密计算机、涉密存储设备赠送、出售、丢弃或改作其他用途。第二十六条规定，禁止非法复制、记录、存储国家秘密；禁止在互联网及其他公共信息网络或未采取保密措施的有线和无线通信中传递国家秘密；禁止在私人交往和通信中涉及国家秘密。《网络安全法》第四章“网络信息安全”涉及对公民个人信息、隐私和企业商业秘密的保护，相比《保密法》前款内容，又加大了公民个人信息、隐私和企业商业秘密安全保护的力度。在此基础上，两法将国家安全与公民个人信息，隐私和企业商业秘密纳入法律保护体系。

#### 5. 《网络安全法》与《刑法》

在应对危害网络安全活动的专业性、技术性强等特点上，单独针对任何单一或部分行为的打击或治理无法实现对“产业链”的全方位覆盖。因此，《刑法》作为抗御社会违法行为的最后一道防线，其严格把握“入罪”的界限，通过多次修正案不断调整思路，对危害网络安全活动也做了相关规定。第二百八十五条规定了非法侵入计算机信息系统罪；非法获取计算机信息系统数据、非法控制计算机信息系统罪；提供侵入、非法控制计算机信息系统程序、工具罪。第二百八十六条规定了破坏计算机信息系统罪；网络服务渎职罪。第二百八十七条规定了利用计算机实施犯罪的提示性规定。此外，《刑法修正案（九）》针对《刑法》第二百八十五条的规定增加了单位犯罪的情形；在《刑法》第二百八十六条中增加了拒不履行信息网络安全管理义务罪和前款的单位犯罪的情形；在《刑法》第二百八十七条后增加了非法利用信息网络罪，帮助信息网络犯罪活动罪及单位犯罪的情形，进一步加强网络空间活动的监管，加大对危害网络安全行为的惩处力度，维护网络空间安全运行。《网络安全法》作为从预防到惩治的综合性立法，也适时提出了多方参与、综合治理的构想，丰富了《刑法》原本的对侵入系统、窃取数据等罪名的行为规定，对预防和惩罚犯罪有着不可替代的意义。

《网络安全法》第二十七条将危害网络安全运行行为分为三大类，包括危害网络安全的活动；提供危害活动的程序及工具的帮助行为；提供技术支持、广告推

广、支付结算的帮助。危害网络安全的活动又细分为非法侵入他人网络、干扰他人网络正常功能、窃取网络数据，这和《刑法》的规定基本吻合，《刑法》及其司法解释中详细规定了行为构成要件和惩罚制度。其中，侵入行为主要通过各种非授权访问的方式进入网络、系统，直接危害网络运行和网络数据的保密性、完整性；干扰行为则主要通过各种物理或逻辑的方式导致网络、系统的功能紊乱、错误、丧失，直接危害网络运行和系统的完整性、可用性；窃取网络数据的行为通常发生在侵入行为之后，对象可以包括一般数据和敏感、涉密数据，如隐私、商业秘密和国家秘密等信息，主要危害网络数据的保密性和可用性（严格而言，随着实施危害活动的程序和工具的能力强化，某一危害行为均可能同时危害保密性、完整性和可用性，并在行为和危害后果上难以截然区分如利用勒索软件实施的攻击行为）。危害网络安全的活动、提供危害活动的程序及工具这两种行为的主观态度应当包括故意或过失，提供技术支持、广告推广、支付结算的帮助行为则明确指出行为人应为故意，即“明知”。

将《网络安全法》与现有《刑法》进行对比可以看出，《网络安全法》也做出了进一步细化规定。

首先，《网络安全法》构建了涵盖事先监测预警、事中应急响应、事后惩治与恢复的“三位一体”的治理体系。基于网络攻击的低成本性、隐藏性及影响范围广等特征，仅仅依靠事后惩治显然不能起到对网络攻击的威慑，更难以实现对网络安全的保障。我国《刑法》第二百八十五条、第二百八十六条、第二百八十七条规制的行为是已经实施的入侵计算机信息系统的行为，或者造成实体损害的行为。显然其作用只是起到了对犯罪行为人的处罚，对于已经造成的损害无法进行弥补。而《网络安全法》“三位一体”的治理体系，从源头对网络攻击进行防范，在攻击发生时确保能够迅速响应与处置，将损害降至最低，最后再对犯罪行为人进行惩处。《网络安全法》规定网络运营者应当制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险；在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告；此外，还明确要求国家也要建立网络安全监测预警和信息通报制度。

其次，《网络安全法》建立了信息共享机制，确保信息的及时、准确。近年来，我国在信息公开方面做出了许多努力，而《刑法》在经过 2015 年第九次修订后尚



未增加网络安全信息共享的内容。《网络安全法》作为网络安全领域的基本法对该部分内容进行了完善与补充,明确规定国家网信部门应当统筹协调有关部门对关键信息基础设施的安全保护采取下列措施:促进有关部门、关键信息基础设施运营者,以及有关研究机构、网络安全服务机构等之间的网络安全信息共享。

再次,《网络安全法》保护与规制的范围较之《刑法》更加广泛。依据《刑法》第二百八十五条第一款的规定,国家事务、国防建设、尖端科学技术领域是关键基础设施领域的重要组成部分。显然,仅依靠这部分的安全并不能实现真正的网络安全。而《网络安全法》对这方面的规定就更加全面和科学。设立“关键信息基础设施的运行安全”专门章节对关键信息基础设施进行统一且全面的规定。

最后,《网络安全法》新增了漏洞披露等规定。目前,安全漏洞攻击成为全球网络安全最大的威胁之一。作为网络大国的中国,也亟须提升防御能力,最大限度减少安全漏洞可能产生的危害。我国《刑法》仅在第二百八十五条、第二百八十六条、第二百八十七条规定了关于入侵计算机信息系统的犯罪,并未明确漏洞挖掘、披露等内容。《网络安全法》要求开展网络安全认证、检测、风险评估等活动,向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息,并规定了相应的惩罚责任。

可以看出,在借鉴国际经验、结合我国国情的情况下,在应对各类突发网络安全攻击事件方面,《网络安全法》都是对《刑法》的一大突破。构建“三位一体”治理体系,对关乎民生的重要领域的网络安全重点保护都顺应了社会的发展趋势,其中网络安全信息共享与漏洞更是一个新亮点。考虑到《网络安全法》的网络安全领域基本法的地位,只能从宏观上对网络安全治理进行原则上的规定,为了确保法律的效力和实施效果,还需要制定相配套的立法与之相结合,共同提升我国网络安全治理水平。

### 第三节 《网络安全法》的基本原则

法的原则是法的灵魂,是指导整个法律活动的核心思想,是实现法的目的的基本保证。《网络安全法》的原则是贯穿互联网安全立法、司法、执法环节,实现

维护社会公共安全的法制目的的根本规则。《网络安全法》是我国第一部全面规范网络空间安全治理问题的基础性法律，无论是从立法宏观思路还是从具体制度设计上都具有全局性、战略性及实践性。在基本原则层面，《网络安全法》的“灵魂”聚焦于以下几个层面。

## 一、网络空间主权原则

由于网络空间不断扩展着国家安全空间，改变了国家间的权力博弈方式，世界强国围绕网络治理展开了非常激烈的博弈。由于各大国在网络核心资源、核心技术的市场占有份额及文化价值观念等方面的差异，网络空间的治理思路仍存在分歧和矛盾。尤其是网络的跨国界性、去中心化使传统的“主权”边界趋于模糊，同时“网络自由主义”不断兴起，成为网络强国挑衅他国网络主权的得力工具。美国关于网络治理的“全球公域说”及“多利益攸关方模式”不断挑衅着中国政府主导的、建立在网络主权基础上的“多边主义模式”。基于此背景，“网络空间主权原则”正式从学术研究范畴迈入立法视野，成为我国网络空间治理的基本原则。

《国家安全法》第二十五条规定，加强网络管理，防范、制止和依法惩治网络攻击、网络入侵、网络窃密、散布违法有害信息等网络违法犯罪行为，维护国家网络空间主权、安全和发展利益。继此之后，《网络安全法》进一步明确和细化了网络空间主权原则。《网络安全法》第一条规定，为了保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展，制定本法；第二条规定，在中华人民共和国境内建设、运营、维护和使用网络，以及网络安全的监督管理，适用本法；第四条规定，国家制定并不断完善网络安全战略，明确保障网络安全的基本要求和主要目标，提出重点领域的网络安全政策、工作任务和措施；第五条规定，国家采取措施，监测、防御、处置来源于中华人民共和国境内外的网络安全风险和威胁，保护关键信息基础设施免受攻击、侵入、干扰和破坏，依法惩治网络违法犯罪活动，维护网络空间安全和秩序。以上规定体现了习近平总书记在第二届世界互联网大会上代表中国提出的推进全球互联网治理体系变革“四项原则”中的“尊重网络主

权原则”。网络空间主权原则根植于《联合国宪章》和国际法法理，是传统主权在网络空间的自然延伸，表明作为国际法义务主体之国家既享有主权权利又应承担国际法义务。从立法层面确立网络空间的主权原则，既能体现各国政府依法治理网络空间的责任与权利，也有助于推动各国构建政府、企业和社会团体之间良性互动的平台，为信息技术的发展及国际交流与合作营造一个健康的生态环境。

## 二、网络安全与发展并重原则

我国《网络安全法》第三条明确规定，国家坚持网络安全与信息化发展并重，遵循积极利用、科学发展、依法管理、确保安全的方针，推进网络基础设施建设和互联互通，鼓励网络技术创新和应用，支持培养网络安全人才，建立健全网络安全保障体系，提高网络安全保护能力。网络安全与发展并重原则已经成为我国网络法的核心性原则，习近平总书记对安全和发展的关系有着深刻的论述。2016年“4·19”讲话中，习近平总书记指出，网络安全和信息化是相辅相成的。安全是发展的前提，发展是安全的保障，安全和发展要同步推进。

信息技术发展的负面效应给网络空间带来棘手的安全隐患，对安全价值的追求成为我国网络安全治理的目标之一，“没有网络安全就没有国家安全”成为广泛的共识。但是，网络发展的加速度不能因对网络安全的追求而限制并阻碍网络的发展，保守和封闭的安全观难以确保整体国家安全，相反将引发更为广泛和严重的安全隐患。因而，“发展才是硬道理”，网络安全的发展是解决网络安全隐患的基本前提条件，越发频繁的网络安全隐患只有通过网络的不断发展来加以应对和化解，越来越多的网络安全漏洞、黑客攻击和信息泄露事件正在为安全防御能力的提升和治理手段的完善提供丰富的实践案例和经验教训，任何封闭与停滞的观念和治理方式都将给网络发展带来阻力。网络技术的不断发展意味着我们将拥有更为先进的技术、产业，以及培养出成千上万的网络安全顶级人才，最终促进安全。同样，仅追求网络技术的发展而忽略了安全的考量也是不可持续的发展，不能以网络安全的失控为代价去换取一时的经济增长，这与以人为本和科学发展的观念相背离。综上，网络发展与网络安全应统筹兼顾、相互促进，以发展促安全，以安全保发展，努力追求“双轮驱动、两翼齐飞”。

### 三、网络安全风险防御原则

安全风险预防为主原则，是预防为主、防治结合、综合治理原则的简称，其基本内涵是指：国家在网络空间和信息安全保护过程中采取各种技术防范措施，完善各项管理制度，规范信息安全教育，关注信息安全活动中技术、管理、社会、经济和法律之间的关系，以法的强制性防范国家信息化建设过程中出现的各种安全风险。我国《网络安全法》基本制度的设定集中体现了网络安全风险防御的原则。《网络安全法》第三章“网络运行安全”和第五章“检测预警与应急处置”的条款设置体现了网络安全风险防御的思想。第二十五条规定，网络运营者应当制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险；在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告。第五十一条规定，国家建立网络安全监测预警和信息通报制度。国家网信部门应当统筹协调有关部门加强网络安全信息收集、分析和通报工作，按照规定统一发布网络安全监测预警信息。

随着云计算、大数据、移动互联网等新兴技术的广泛应用，网络已由独立分散走向深度关联、相互依赖。随着系统边界的模糊，安全威胁样式及黑客攻击手段不断发生变化。动态、综合的网络安全风险防御理念急需树立并应用于实践。

《网络安全法》采用风险防御原则，有利于强化国家对网络安全风险的控制。网络安全风险是当代社会所面临的巨大风险。由于网络本身的脆弱性，人们还不能只依赖技术措施防范网络安全风险，必须采取综合治理的方式，将“风险预防原则”落实在网络建设、使用、运营的每个环节。如果每个参与网络的活动者都能够树立网络安全意识，注意网络安全道德修养，掌握网络安全知识，明确网络安全责任，那么，我们就能将网络安全风险降低到最低程度，以维护国家安全，保障社会公共安全和保护网络参与者的合法利益。

### 四、协同治理原则

协同理论是现代系统科学理论体系的一支，由德国著名理论物理学家赫尔曼·

哈肯在1970年创立。协同理论认为,系统要素在各自发挥作用时,必须借助于其他系统条件,假如能得到其他条件的配合,则可以发挥其应有的作用,反之则可能削弱其功效。网络安全的协同治理是指应充分发挥包括政府部门、执法机关、社会组织、企业及公民个人在内的每个社会单元的力量,以实现责任分担、协同参与及利益共享。尤其是应重视企业及政府在网络攻击法律治理中的主导作用,不仅要求各主管部门和应急机构不断整合自身的优势,明确职能分工,最终形成合力,还应充分发挥企业尤其是网络服务提供者在网络攻击防御与控制中的“一线”优势。我国《网络安全法》在关键信息基础设施保护、个人信息保护、网络安全风险监测预警、应急相应制度建立中尤为重视国家政府、行业管理部门、企业、社会组织及个人发挥的协同作用。实际上,网络空间安全仅仅依靠政府是无法实现的,而是需要政府、企业、社会组织、技术社群和公民等网络利益相关者的共同参与。《网络安全法》坚持共同治理原则,要求采取措施鼓励全社会共同参与,政府部门、网络建设者、网络运营者、网络服务提供者、网络行业相关组织、高等院校、职业学校、社会公众等都应根据各自的角色参与网络安全治理工作。

## 第四节 《网络安全法》的调整对象

### 一、《网络安全法》调整对象的界定

任何法律规范都有其特定的调整对象,即某种特定的社会关系。社会关系自身的内在联系和不同社会关系的彼此差异,构成了法的独立调整对象,是划分法的部门的基础。《网络安全法》的调整对象是网络安全保障法律关系,即国家在保障网络安全,维护网络空间主权和国家安全、社会公共利益,保护公民、法人和其他组织合法权益的过程中所形成的社会关系。值得注意的是,网络安全保障关系集中表现为网络安全监督管理关系,其中涵盖诸多方面:第一,国家网信部门与国家工信、公安、国家安全、国家保密行政管理、国家密码管理等政府相关部门及网络运营者之间的网络安全统筹协调和监督管理关系;第二,中央政府有关部门与地方政府有

关部门之间针对网络安全保障相关事项的上下级领导和监督管理关系；第三，政府有关部门（通常为行业主管或监管部门）与网络运营者之间的网络安全监督管理关系。具体而言，网络安全保障关系的内容不仅包括网络运营者、关键信息基础设施运营者、网络产品和服务提供者、行业组织和个人等在建设、运营、维护和使用网络的过程中享有的法定权利和应当履行的法定义务，还包括国家网信、工信、公安、国家安全、国家保密行政管理、国家密码管理等政府相关部门在履行网络安全保护和监督管理职责的过程中依法享有的职权和应当履行的职责。

## 二、《网络安全法》调整对象的内容

《网络安全法》的调整对象具体包括以下几个方面。

### （一）关键信息基础设施保护监督管理关系

《网络安全法》重点关注关键信息基础设施保护的运行安全，并建立了关键信息基础设施安全保护的工作部门与本行业、本领域关键信息基础设施运营者之间，针对关键信息基础设施安全保护工作的指导和监督管理关系，以及国家网信部门与有关部门的关键信息基础设施保护统筹协调关系。在此基础上，《关键信息基础设施安全保护条例》进一步建立了国家网信部门与国务院公安、国家安全、国家保密行政管理、国家密码管理等部门之间，针对关键信息基础设施安全保护工作的统筹协调和监督管理关系；中央政府有关部门与地方政府有关部门之间，针对关键信息基础设施安全保护工作的上下级领导和监督管理关系；国家网信部门与关键信息基础设施运营者、有关研究机构、网络安全服务机构等之间，针对网络安全信息共享建立的统筹协调关系；国家行业主管或监管部门与本行业、本领域关键信息基础设施运营者之间的指导和监督管理关系。

### （二）网络安全等级保护监督管理关系

《网络安全法》第二十一条以网络安全领域基本法的形式确立了网络安全等级保护制度，规定了等级保护制度安全措施的基线要求并赋予其强制力。同时，第三十一条进一步要求关键信息基础设施保护必须落实国家网络安全等级保护制度，突出

保护重点。由此可见，网络安全等级保护制度建立了公安、国家保密行政管理、国家密码管理等政府相关部门与网络运营者之间的网络安全等级保护监督管理关系。

### （三）网络安全检测、认证、风险评估的监督管理关系

《网络安全法》鼓励有关企业、机构开展网络安全认证、检测和风险评估等安全服务，但要求开展网络安全认证、检测、风险评估等活动应当遵守国家有关规定。由此可见，国家网信、工信、公安、国家保密行政管理、国家密码管理等政府相关部门针对有关企业、机构进行网络安全检测、认证、风险评估的监督管理关系也构成《网络安全法》的调整对象。

### （四）网络用户身份管理法律关系

《网络安全法》明确要求落实网络实名制，在此基础上建立了国家网信、工信、公安等政府相关部门与基础电信运营商、网络信息服务提供者等网络运营者及网络用户之间的网络用户身份管理法律关系。

### （五）网络安全监控法律关系

基于维护国家安全和侦查犯罪的现实需求，《网络安全法》将公安机关、国家安全机关与网络运营者之间的网络安全监控法律关系纳入其调整范围。

### （六）网络安全漏洞披露法律关系

作为网络安全风险控制的中心环节，网络安全漏洞披露对降低风险和分化风险起着至关重要的作用，向不特定的社会公众披露网络安全漏洞可以提升网络安全防护的实时性和有效性，但恶意或非法的网络安全漏洞披露同样为攻击者提供了可利用的攻击武器。国家网信、工信、公安等政府相关部门在此过程中与网络安全服务机构、网络运营者、网络产品和服务提供者，以及社会公众之间形成了网络安全漏洞披露法律关系。

### （七）网络产品和服务监督管理关系

网络产品和服务在研发、生产、运维过程中可能产生很多安全问题，包括产

产品和服务自身的安全风险，以及被非法控制、干扰和中断运行的风险；产品及关键部件生产、测试、交付、技术支持过程中的供应链安全风险；产品和服务提供者利用提供产品和服务的便利条件非法收集、存储、处理、使用用户相关信息的风险；产品和服务提供者利用用户对产品和服务的依赖，损害网络安全和用户利益的风险等。为了有效降低信息泄露、数据篡改、服务中断、非法远程控制等安全风险，保障网络产品和服务安全，国家网信、工信、公安等政府相关部门在对网络产品和服务安全性、可控性进行安全审查和监督管理的过程中与网络产品和服务提供者之间形成了网络产品和服务监督管理关系。

#### （八）个人信息保护法律关系

随着网络信息技术的快速发展，无孔不入的个人信息收集和使用行为，不可避免地引发个人信息泄露和滥用的问题。国家网信、工信、公安等政府相关部门针对个人信息的收集和使用规范与网络运营者、关键信息基础设施运营者、网络产品和服务提供者，以及网络用户之间形成了个人信息保护法律关系。

#### （九）网络非法有害信息的防治管理关系

加大对互联网“非法有害信息”的监督管理是当前网络社会信息内容治理工作的重要环节，我国目前已经建立了国家网信办、工信部、公安部、文化部、新闻出版广电总局、工商总局等政府相关部门在各自职责范围内，针对网络非法有害信息内容防治事项与地方政府相关部门、网络运营者之间的监督管理关系，以及网络运营者、电子信息发送服务提供者、应用软件下载服务提供者与网络用户之间的网络非法有害信息防治管理关系。

#### （十）网络安全监测预警和信息通报监督管理关系

为了协调国家有关部门及关键信息基础设施行业、领域网络安全监测预警和信息通报工作的协同性和一致性，《网络安全法》建立了国家网信部门与有关部门针对网络安全信息收集、分析和通报工作的统筹协调关系；负责关键信息基础设施安全保护工作的部门与本行业、本领域的关键信息基础设施运营者之间针对网络安全监测预警和信息通报工作的指导和监督管理关系；省级以上政府有关部门



与其他有关部门、机构和人员之间针对网络安全信息收集、报告，网络安全风险监测、评估，以及网络安全风险预警、发布工作的指导和监督管理关系。

#### （十一）网络安全应急保障监督管理关系

为了有效应对网络突发事件，快速响应网络安全风险并将其可能导致的损害降至最低程度，《网络安全法》建立了国家网信部门与有关部门针对网络安全风险评估和应急处置工作的统筹协调关系；负责关键信息基础设施安全保护工作的部门与本行业、本领域的关键信息基础设施运营者之间的网络安全应急保障监督管理关系；国家网信部门和地方政府有关部门与网络运营者之间的网络安全应急指导和监督管理关系。

#### （十二）网络安全国际治理关系

《网络安全法》鼓励和倡导国家积极开展网络空间治理、网络技术研发和标准制定、打击网络违法犯罪等方面的国际交流与合作，推动构建和平、安全、开放、合作的网络空间，建立多边、民主、透明的网络治理体系。习近平总书记提出的“深化网络空间国际合作，携手构建网络空间命运共同体”主张，充分表明维护网络空间的开放、共享、和平和稳定符合世界各国的共同利益。因此，网络安全国际治理关系也是《网络安全法》的调整对象之一。

### 第五节 《网络安全法》的行为准则

人类的行为看起来复杂多样，变幻莫测，似乎没有什么规律可循，但整个社会又井然有序、由低级向高级、由简单到复杂、不断向前发展。这说明，任何一个社会都必然存在各种形式的具体约束规则来制约和控制个人和集体的行为。行为准则即为个人、集体或社会的行为所服从的约束条件。根据约束条件不同，行为准则可以分为两大基本类型：一是提倡性行为准则，又称为“应该”型行为准则，其本质在于倡导和鼓励个人、集体、社会甚至国家实施能够产生最大正向价

值效应的行为；二是限制性行为准则，又称为“不能”型行为准则，其本质在于限制或禁止个人、集体、社会甚至国家实施产生最大负向价值效应的行为。随着网络空间成为人类社会第二类生存空间和第五大作战领域，关于网络空间安全行为准则的制定显得尤为必要。

## 一、国家层面的网络空间行为准则

### （一）国家层面对外的网络空间行为准则

国家层面对外的网络空间行为准则旨在明确国家在网络空间的权利与责任，推动国家在网络空间实施建设性和负责任的行为，促进国家间在应对网络安全威胁与损害时积极合作并不断努力构建和平、安全、开放、合作的网络空间，坚持维护国际和平与安全的目的，尽力促进人类社会和经济全面发展及人类福祉。

#### 1. 维护国家网络空间主权

互联网发展不能有违以《联合国宪章》为基础的国际法和国际关系基本准则，国家主权原则在网络空间同样适用。国家对其领土内的网络基础设施，以及建设、运营、维护和使用网络活动拥有管辖权。

各国应当遵守《联合国宪章》和公认的国际关系基本准则，包括尊重各国主权尤其是网络空间主权、领土完整和政治独立，尊重人权和基本自由，尊重各国历史、文化、社会制度的多样性等。

各国应努力确保信息技术产品和服务供应链的安全，防止他国利用优势，削弱本国对信息技术的自主控制权，或者威胁国家政治、经济和社会安全。

任何国家有权依法保护本国网络空间及关键信息基础设施安全，使其免受威胁、干扰、攻击和破坏。

#### 2. 规范网络空间活动，积极履行国家职责与义务

各国应和平利用网络空间，不得利用网络和信息通信技术干涉他国内政，破坏他国政治、经济和社会稳定，损害他国利益。

各国不得利用网络和信息通信技术实施有悖于维护国际和平与安全目标的

活动。

各国应致力于共同打击利用网络和信息通信技术从事犯罪和恐怖活动，或者传播宣扬恐怖主义、分裂主义、极端主义的信息，或者其他破坏他国政治、经济和社会稳定，以及精神文化环境信息的行为。

### 3. 充分尊重个人在网络空间的权利与自由

各国应充分尊重个人在网络空间的权利和自由，包括在遵守各国法律法规的前提下寻找、获得、传播信息的权利和自由。

### 4. 促进国际合作及网络治理秩序的完善

各国应在相互尊重、平等互利的基础上，共同构建和平、安全、开放、合作的网络空间。

各国应推动建立多边、透明和民主的国际网络治理机制，促进网络相关资源的公平分配，并确保互联网的稳定安全运行。

各国政府应与各利益攸关方充分合作并不断促进、创建网络安全文化的形成与交流。

各国应致力于共同打击网络犯罪活动，加强国际司法与执法合作，促进国际合作与经验交流。

各国应制定务实的建立信任措施，尽力防止国家间的网络安全冲突。

各国应加强双边、区域和国际合作。推动联合国在促进制定网络安全国际法律规范、和平解决相关争端、促进各国合作等方面发挥重要作用，加强相关国际组织之间的协调。

各国应确保在涉及上述准则的活动时产生的任何争端，都以和平方式解决，不得使用武力或以武力相威胁。

## （二）对内的网络空间行为准则

国家层面对内的网络空间行为准则主要涉及公权力机关代表国家履行网络安全监督管理职责，保障本国网络运行安全、网络信息安全，支持网络安全技术发展等，并不断在以下事务方面履行职责。

坚持网络安全与信息化发展并重。

遵循积极利用、科学发展、依法管理、确保安全的方针。

推进网络基础设施建设和互联互通。

鼓励网络技术研究与应用。

增加教育、科研投入，支持培养网络安全人才。

建立健全网络安全保障体系，提高网络安全保护能力。

重点保护关键信息基础设施安全。

依法惩治网络违法犯罪活动，维护网络空间安全和秩序。

采取措施提高全社会的网络安全意识和水平。

保护公民、法人和其他组织依法使用网络的权利。

促进网络资源公平、合理分配。

推进网络安全社会化服务体系建设，鼓励有关企业、机构开展网络安全认证、检测和风险评估等安全服务。

促进网络空间法治建设，完善网络安全法治体系。

推进法律、法规及政策落实。

确保公权力机关依法行政。

提高打击网络犯罪活动的的能力。

提高网络攻击、网络威胁的应对能力。

## 二、产业层面的网络空间行为准则

产业层面的网络空间行为准则主要约束在一国从事建设、运营、维护、使用网络的活动，该行为准则针对的主体为网络运营者、网络产品和服务提供者、关键信息基础设施运营者，以及网络安全服务机构等，其主要内容包括以下方面。

自觉遵守国家有关互联网发展和管理的政策和法律法规，遵守国家强制标准及行业标准，努力加强行业自律。

尊重社会公德，遵守商业道德，诚实信用。

接受政府和社会的监督，积极承担和践行企业社会责任。

合法、公平、有序竞争，不得实施不正当竞争或垄断行为。

积极落实网络安全保障义务。

自觉维护消费者、用户的合法权益。

尊重他人知识产权及其他合法权益。

保护未成年人上网权益及身心健康发展。

共同防范背离网络安全目的的行为，尤其是网络犯罪活动、恐怖活动等。

加强沟通协作，研究、探讨我国互联网行业发展战略，对我国互联网行业的建设、发展和管理建言献策。

支持采取各种有效方式，开展互联网行业科研、生产及服务等领域的协作，共同创造良好的行业发展环境。

积极参加国际交流与合作，参与行业国际规则的制定，自觉遵守我国签署的国际规则。

### 三、个人层面的网络空间行为准则

个人层面的网络空间行为准则主要约束个人运营、维护和使用网络的活动，该行为准则针对的主体涉及安全从业者、履行网络安全监督管理职责的工作人员，以及普通用户，其主要内容包括以下方面。

任何个人和组织使用网络应当遵守宪法法律，遵守公共秩序，尊重社会公德，不得危害网络安全，不得利用网络从事危害国家安全、荣誉和利益，煽动颠覆国家政权、推翻社会主义制度，煽动分裂国家、破坏国家统一，宣扬恐怖主义、极端主义，宣扬民族仇恨、民族歧视，传播暴力、淫秽色情信息，编造、传播虚假信息扰乱经济秩序和社会秩序，以及侵害他人名誉、隐私、知识产权和其他合法权益等活动。

任何个人和组织不得从事非法侵入他人网络、干扰他人网络正常功能、窃取网络数据等危害网络安全的活动；不得提供专门用于从事侵入网络、干扰网络正常功能及防护措施、窃取网络数据等危害网络安全活动的程序、工具；明知他人从事危害网络安全的活动的，不得为其提供技术支持、广告推广、支付结算等帮助。

任何个人和组织不得窃取或以其他非法方式获取个人信息，不得非法出售或非法向他人提供个人信息。

依法负有网络安全监督管理职责的部门及其工作人员，必须对在履行职责中知悉的个人信息、隐私和商业秘密严格保密，不得泄露、出售或非法向他人提供。

任何个人和组织应当对其使用网络的行为负责，不得设立用于实施诈骗，传授犯罪方法，制作或销售违禁物品、管制物品等违法犯罪活动的网站、通信群组，不得利用网络发布涉及实施诈骗，制作或销售违禁物品、管制物品及其他违法犯罪活动的信息。

任何个人和组织发送的电子信息、提供的应用软件，不得设置恶意程序，不得含有法律、行政法规禁止发布或传输的信息。

应当提高网络安全意识与风险意识。

应当尊重他人商业秘密、知识产权、个人隐私等合法权益。

应当合理利用网络资源。

## 第二部分

# 一般网络运营者的网络安全法律遵从

第 5 章 网络安全等级保护制度

第 6 章 实名制与可信身份战略

第 7 章 网络安全监测预警和应急响应

第 8 章 安全认证、检测及风险评估

第 9 章 网络安全信息披露

第 10 章 协助执法

第 11 章 个人信息保护

第 12 章 网络信息内容过滤





# 网络安全等级保护制度

随着网络普及化程度的日益提升，云计算、大数据、物联网等新一代信息技术的迅速发展，网络安全威胁态势日益严峻，网络安全问题成为我国乃至全球重点关注的问题。网络安全等级保护制度是我国保障网络安全的一项基本制度，以所承载的业务应用的“社会重要性”来确定安全保护等级，对不同等级的系统采用不同的“基线”予以保护并对其实施不同的监管。实行网络安全等级保护制度，能够充分调动国家、法人和其他组织及公民的积极性，发挥各方面的作用，达到有效保护的目的，增强安全保护的整体性、针对性和实效性。作为我国首部网络安全领域的基本法律，《网络安全法》首次将网络安全等级保护制度从一项基本制度、基本国策上升到法律层面。

## 第一节 《网络安全法》相关规定及释义

总体来说，《网络安全法》让我国作为基本国策的信息安全等级保护制度在基本法层面确立为网络安全等级保护制度，以“保障网络免受干扰、破坏或未经授权的访问，防止网络数据泄露或被窃取、篡改”为根本目的，规定了等级保护制度安全措施基线要求并赋予强制力。

在《网络安全法》中，网络安全等级保护制度体现为第二十一条和第五十九

条。第二十一条规定国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或未经授权的访问，防止网络数据泄露或者被窃取、篡改：①制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；②采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施；③采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于6个月；④采取数据分类、重要数据备份和加密等措施；⑤法律、行政法规规定的其它义务。

第五十九条规定的主要是法律责任，即网络运营者不履行本法第二十一条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或导致危害网络安全等后果的，处一万元以上十万元以下罚款，对直接负责的主管人员处五千元以上五万元以下罚款。

从《网络安全法》第二十一条的规定来看，网络安全等级保护制度保护的对象既包括信息系统，也包括信息系统中存在的网络数据。网络安全等级保护制度将网络运营者作为第一责任人，要求网络运营者根据网络安全等级保护制度的要求，采取相应的管理措施和技术防范等措施，履行相应的网络安全保护义务。义务内容方面，《网络安全法》针对一般网络运营者与关键信息基础设施的网络运营者在安全等级保护制度下设置了不同程度的安全保障义务。一般网络运营者仅需遵从第二十一条规定的安全保障义务。关键信息基础设施网络运营者除了第二十一条规定的义务外还需遵守第三十四条的规定。法律责任方面，承担责任的主体不仅包括网络运营者，还包括直接负责的主管人员，处罚方式包括责令改正后警告和罚款。其中责令改正后警告属于未造成危害后果的前置条件，拒不改正后进一步做出罚款处罚；在网络运营者不履行安全保护义务导致危害网络安全后果的情形下，可直接做出罚款处罚。以下是具体释义。

## 一、义务主体

根据《网络安全法》第二十一条的规定，网络安全等级保护制度的义务主体是“网络运营者”。第七十六条对网络运营者的概念进行了界定，认为“网络运营者”

是指网络的所有者、管理者和网络服务提供者。

在《网络安全法》颁布之前，网络运营者的概念仅在已经失效的《电信服务标准（试行）》中出现过，但在该规定中“网络运营者”主要是指提供通道、电路段的网络服务提供商，与《网络安全法》中的网络运营者并非同一概念。根据《网络安全法》对于网络的定义，这里规定的网络既包括电信网、广播电视传输网、互联网等基础信息网络，也包括局域网、工业控制系统等不向社会提供商业或公共服务的网络。网络所有者、网络管理者则是指前述信息系统的所有者和管理者。网络服务提供者指的则是依托于网络这个信息系统的各类服务提供者，网络服务包括了网络信息服务、网络接入服务及其他网络服务。因此，网络安全等级保护制度下安全保障义务的网络运营者的范畴相当广泛，既包括如移动、联通、电信等基础电信网络的所有者和管理者，也包括像京东、腾讯、新浪等这样的网络信息服务提供者；既包括经营性的网络服务运营者，也包括非经营性的网络运营者；既包括向公众提供服务的互联网的运营者，也包括不向公众提供服务的局域网或工业控制系统的运营者。

## 二、义务内容

网络安全等级保护制度下，《网络安全法》从管理措施和技术措施两个层面规定了网络运营者的义务。具体来说，网络运营者的主要义务包括以下内容。

### （一）制定内部安全管理制度及操作规程

根据等级制度的要求，网络运营者应制定内部安全管理制度和操作规程，对安全管理活动中的主要管理内容建立安全管理制度，对要求管理人员或操作人员执行的日常管理操作建立操作规程。安全管理制度应通过正式、有效的方式发布，并进行版本控制，应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。

网络安全等级保护的核心是保证不同安全保护等级的对象具有相适应的安全保护能力。《信息系统安全等级保护基本要求》（GB/T 22239—2008）对不同安全保护等级对象的安全管理制度提出了不同强度的基本要求，网络运营者可以参考。

## （二）确定网络安全负责人

网络运营者应根据不同保护等级设立信息安全管理工作的职能部门，设立安全主管、安全管理各方面的负责人岗位，并明确各负责人的职责；应设立系统管理员、网络管理员、安全管理员等岗位，并明确各工作岗位的职责；应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施。《信息系统安全等级保护基本要求》（GB/T 22239—2008）对不同安全保护等级对象的安全管理机构 and 人员安全管理等提出了不同强度的基本要求，网络运营者可以参考。

## （三）采取防范危害网络安全行为的技术措施

为落实网络安全等级保护制度，网络运营者应当采取技术防范措施，防范计算机病毒和网络攻击、网络侵入等网络安全风险。《网络安全法》之外，《计算机信息网络国际联网安全保护管理办法》<sup>①</sup>、公安部发布的《互联网安全保护技术措施规定》<sup>②</sup>等规定中对于网络运营者应该承担的技术措施做出了规定。网络运营者应当采取的技术措施包括安装防病毒软件，防范计算机病毒；安装网络身份认证系统、网络入侵检测系统、网络风险审计系统等，防范网络攻击、侵入等。《信息系统安全等级保护基本要求》（GB/T 22239—2008）规定了不同安全保护等级对象

① 《计算机信息网络国际联网安全保护管理办法》第十条规定，互联单位、接入单位及使用计算机信息网络国际联网的法人和其他组织应当履行落实安全保护技术措施，保障本网络的运行安全和信息安全的安全职责。

② 《互联网安全保护技术措施规定》第七条规定，互联网信息服务提供者和联网使用单位应当落实以下互联网安全保护技术措施：①防范计算机病毒、网络入侵和攻击破坏等危害网络安全事项或行为的技术措施；②重要数据库和系统主要设备的冗余备份措施；③记录并留存用户登录和退出时间、主叫号码、账号、互联网地址或域名、系统维护日志的技术措施；④法律、法规和规章规定应当落实的其他安全保护技术措施。第八条规定，提供互联网接入服务的单位除落实本规定第七条规定的互联网安全保护技术措施外，还应当落实具有以下功能的安全保护技术措施：①记录并留存用户注册信息；②使用内部网络地址与互联网网络地址转换方式为用户提供接入服务的，能够记录并留存用户使用的互联网网络地址和内部网络地址对应关系；③记录、跟踪网络运行状态，监测、记录网络安全事件等安全审计功能。第九条规定，提供互联网信息服务的单位除落实本规定第七条规定的互联网安全保护技术措施外，还应当落实具有以下功能的安全保护技术措施：①在公共信息服务中发现、停止传输违法信息，并保留相关记录；②提供新闻、出版及电子公告等服务的，能够记录并留存发布的信息内容及发布时间；③开办门户网站、新闻网站、电子商务网站的，能够防范网站、网页被篡改，被篡改后能够自动恢复；④开办电子公告服务的，具有用户注册信息和发布信息审计功能；⑤开办电子邮件和网上短信息服务的，能够防范、清除以群发方式发送伪造、隐匿信息发送者真实标记的电子邮件或短信息。第十条规定，提供互联网数据中心服务的单位和联网使用单位除落实本规定第七条规定的互联网安全保护技术措施外，还应当落实具有以下功能的安全保护技术措施：①记录并留存用户注册信息；②在公共信息服务中发现、停止传输违法信息，并保留相关记录；③联网使用单位使用内部网络地址与互联网网络地址转换方式向用户提供接入服务的，能够记录并留存用户使用的互联网网络地址和内部网络地址对应关系。第十一条规定，提供互联网上网服务的单位，除落实本规定第七条规定的互联网安全保护技术措施外，还应当安装并运行互联网公共上网服务场所安全管理系统。

的入侵防范基本要求，网络运营者可以参考。例如，二级要求“应在网络边界处监视以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击和网络蠕虫攻击等”；三级要求“a) 应在网络边界处监视以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击和网络蠕虫攻击等；b) 当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警”。

#### （四）网络监测与日志留存

根据网络安全等级制度的要求，网络运营者应当监测、记录网络运行状态、网络安全事件，并留存相关的网络日志不少于 6 个月。《网络安全法》颁布之前我国的许多规范中已经存在与网络日志留存相关的规定，基本源自 2000 年国务院发布的《互联网信息服务管理办法》规定。《互联网信息服务管理办法》（国务院令 第 292 号）第十四条规定，互联网信息服务提供者应当记录提供的信息内容及其发布时间、互联网地址或域名；互联网接入服务提供者应当记录上网用户的上网时间、用户账号、互联网地址或域名、主叫电话号码等信息。互联网信息服务提供者和互联网接入服务提供者的记录备份应当保存 60 日。

2003 年铁道部发布《铁路计算机信息系统安全保护办法》（铁道部令 第 10 号），第二十七条规定重要计算机信息系统应当建立完善的计算机信息系统日志，根据信息的重要程度设定保存时间，最短不少于 60 日。2006 年公安部发布《互联网安全保护技术措施规定》（公安部令 第 82 号），第十三条规定互联网服务提供者和联网使用单位依照本规定落实的记录留存技术措施，应当具有至少保存 60 日的记录备份的功能。

2012 年工业和信息化部发布《移动互联网恶意程序监测与处置机制》（2018 年 1 月 1 日起废止）<sup>①</sup>，第十二条规定，国家互联网应急中心（National Internet Emergency Center, CNCERT）、移动通信运营企业、互联网域名注册管理机构和注册服务机构应留存所监测和处置的移动互联网恶意程序相关数据或资料以备查验。数据或资料保存时间为 60 日。少数行业规范超出了 60 日的规定，如中国证

<sup>①</sup> 2017 年 8 月 9 日，工业和信息化部关于印发《公共互联网网络安全威胁监测与处置办法》的通知规定，“本办法自 2018 年 1 月 1 日起实施。2009 年 4 月 13 日印发的《木马和僵尸网络监测与处置机制》和 2011 年 12 月 9 日印发的《移动互联网恶意程序监测与处置机制》同时废止”。

券监督管理委员会发布的《中国证券监督管理委员会公告（2011）39号——证券期货业信息系统安全等级保护测评要求（试行）》规定检查审计记录应当至少保存6个月；2009年《商业银行信息科技风险管理指引》第二十七条规定，“系统日志由操作系统、数据库管理系统、防火墙、入侵检测系统和路由器等生成，内容包括管理登录尝试、系统事件、网络事件、错误信息等。系统日志保存期限按系统的风险等级确定，但不能少于一年”。

### （五）数据分类、重要数据备份和加密

随着云计算、大数据等技术的发展和应用，网络数据安全对维护国家安全、经济安全，保护公民合法权益，促进数据利用至关重要。网络安全等级制度要求网络运营者对数据进行分类，重要数据采取备份和加密等措施，防止网络数据被窃取或篡改。

数据分类是按照重要程度等标准对数据进行区分、归类。我国现行的规范中还未有对数据分类标准的具体规定。《信息安全等级保护管理办法》第三十四条规定，国家密码管理部门对信息安全等级保护的密码实行分类分级管理。对于重要数据备份和加密中重要数据的认定问题，《网络安全法》没有做具体的界定。第三十七条<sup>①</sup>关于关键信息基础设施的重要数据出境中有“重要数据”的有关规定。基于《网络安全法》第三十七条，2017年国家互联网信息办公室发布了《个人信息和重要数据出境安全评估办法（征求意见稿）》，定义“重要数据”为与国家安全、经济发展，以及社会公共利益密切相关的数据。从此定义可以看出第三十七条中的“重要数据”的识别需要考量的因素包括国家安全、经济发展和社会公共利益。之后国家标准《信息安全技术 数据出境安全评估指南（征求意见稿）》对重要数据进行了进一步的认定<sup>②</sup>。从上述规定中可以看出，数据出境规范中的“重要数据”

① 第三十七条规定关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定。

② 《信息安全技术 数据出境安全评估指南（征求意见稿）》指出“重要数据”是指我国政府、企业、个人在境内收集、产生的不涉及国家秘密，但与国家安全、经济发展及公共利益密切相关的数据（包括原始数据和衍生数据），一旦未经授权披露、丢失、滥用、篡改或销毁，或者汇聚、整合、分析后，可能造成以下后果：①危害国家安全、国防利益，破坏国际关系；②损害国家财产、社会公共利益和个人合法权益；③影响国家预防和打击经济与军事间谍、政治渗透、有组织犯罪等；④影响行政机关依法调查处理违法、渎职或涉嫌违法、渎职行为；⑤干扰政府部门依法开展监督、管理、检查、审计等行政活动，妨碍政府部门履行职责；⑥危害国家关键基础设施、关键信息基础设施、政府系统信息系统安全；⑦影响或危害国家经济秩序和金融安全；⑧可分析出国家秘密或敏感信息；⑨影响或危害国家政治、国土、军事、经济、文化、社会、科技、信息、生态、资源、核设施等其他国家安全事项的数据。

具有以下特点。第一，重要数据与个人数据并非种属关系，个人数据不属于规范中的重要数据。虽然《信息安全技术 数据出境安全评估指南（征求意见稿）》附录 A “重要数据识别指南”中还增加了对于个人合法利益的考量，疑似可以将个人数据纳入其中，但这与整个指南将个人数据与重要数据分别加以规范的做法并不相符，有待商榷。第二，国家秘密被排除在外，国家秘密的相关规范由其他法律法规进行规定。第三，数据来源为识别要素之一，“重要数据”的来源仅限于境内收集和产生，而不包括来源于境外的数据。

首先，需要注意的是，网络安全等级制度中的“重要数据”与数据出境制度中的“重要数据”略有不同。数据备份、加密与数据出境对于国家安全，社会秩序、公共利益，以及公民、法人和其他组织的合法权益影响的作用方式有所不同。例如，有些用户信息的出境并不会对国家安全、经济发展和社会公共利益产生不利影响，因此不属于数据出境中的“重要数据”。但是对这类数据的备份对于企业自身运营可能具有重大的积极意义，可能就属于网络安全等级保护制度中的“重要数据”。

此外，有些数据的备份可能对网络运营者业务自身运营具有重要意义，因此可能被划分到等级保护中的“重要数据”的范畴，但是此类数据可能因出境对国家安全、经济发展和社会公共利益没有多大影响而被排除在数据出境规范中的“重要数据”的范畴之外。

其次，与数据出境中的“重要数据”强调数据境内产生或收集不同，等级保护制度中的“重要数据”并不区分数据的来源。

最后，在数据出境的规范中，并没有将个人数据纳入重要数据的范畴，而是将个人数据与重要数据分别加以规定和保护。在等级保护制度规定的重要数据加密和备份中并没有另行规定个人数据的保护，鉴于个人数据对于国家、公众或个人的重要意义，等级保护制度中的“重要数据”必然包括个人数据。

综上，等级保护制度中的“重要数据”的认定应当以保护国家安全，社会秩序、公共利益，以及公民、法人和其他组织的合法权益为导向，重点考量数据备份和加密对于网络运营者业务运营的重要意义，以及数据不备份、不加密是否会对国家安全、社会秩序、公共利益，以及公民、法人和其他组织的合法权益造成不利影响。

《信息系统安全等级保护基本要求》（GB/T 22239—2008）规定了不同安全保护等级对象的数据备份要求，网络运营者可以参考。例如，二级对象要求“能够对重要信息进行备份和恢复；提供关键网络设备、通信线路和数据处理系统的硬

件冗余，保证系统的可用性”，三级对象要求“应提供本地数据备份与恢复功能，完全数据备份至少每天一次，备份介质场外存放；应提供异地数据备份功能，利用通信网络将关键数据定时批量传送至备用场地；应采用冗余技术设计网络拓扑结构，避免关键节点存在单点故障；应提供主要网络设备、通信线路和数据处理系统的硬件冗余，保证系统的高可用性”。

值得注意的是，依据《网络安全法》第二十一条的规定，除了制定内部安全管理制度及操作规程、确定网络安全负责人、采取防范危害网络安全行为的技术措施、网络监测与日志留存、数据分类、重要数据备份和加密等明确规定的义务外，法律、行政法规规定的其他义务也是网络运营者需要履行的安全保护义务，如依据《计算机信息系统安全保护条例》第九条和《信息安全等级保护管理办法》第十四条规定的“第三级信息系统应当每年至少进行一次等级测评，第四级信息系统应当每半年至少进行一次等级测评”的义务等。

## 第二节 网络安全等级保护制度概述

### 一、网络安全等级保护制度 1.0 时代

《网络安全法》颁布之前，我国许多规范、文件及标准中已经有对于网络安全等级保护制度的具体规定，但这一时期立法相对分散，立法层级较低，可以称之为网络安全等级保护制度 1.0 时代。

法规政策层面，网络安全等级保护制度初具体系。1994 年，国务院颁布的《计算机信息系统安全保护条例》（国务院令第 147 号）第九条首次明确提出计算机信息系统实行安全等级保护，为我国信息系统实行等级保护提供了法律依据。2003 年，国家信息化领导小组发布《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发〔2003〕27 号），将信息安全等级保护作为国家信息安全保障工作的重中之重，明确指出，信息化发展的不同阶段和不同的信息系统，有着不同的安全需求，要综合考虑网络与信息系统的重要性、涉密程度和面临的信息安全风险等因素，进行相应等级的安全建设和管理。2004 年，公安部、国家保密局、



国家密码管理委员会办公室、国务院信息化工作办公室关于印发《关于信息安全等级保护工作的实施意见》（公通字〔2004〕66号），对信息安全等级保护的基本制度框架进行了规划。根据信息及信息系统的重要程度和危害程度将信息和信息系统的安全保护等级划分为五级：自主保护级、指导保护级、监督保护级、强制保护级、专控保护级。2007年，公安部、国家保密局、国家密码管理局、国务院信息工作办公室联合发布了《信息安全等级保护管理办法》，对信息安全等级保护制度做了较为具体的规定，提出了影响信息安全保护等级定级的两个影响因素：信息系统在国家安全、经济建设、社会生活中的重要程度；信息系统遭到破坏后对国家安全、社会秩序、公共利益，以及公民、法人和其他组织的合法权益的危害程度，并依据上述因素将信息系统的安全保护等级由低到高划分为五个等级。同年，公安部发布的《信息安全等级保护备案实施细则》（公信安〔2007〕1360号）对等级保护的工作做出了具体规定。

标准化层面，网络安全等级制度的标准建设工作初具规模。1999年，国家质量技术监督局发布强制性标准《计算机信息系统安全保护等级划分准则》（GB17859—1999）。该标准将计算机系统安全保护能力划分为用户自主保护级、系统审计保护级、安全标记保护级、结构化保护级、访问验证保护级五个等级，并提出了适用于计算机信息系统安全保护技术能力等级的划分准则，为等级划分和保护奠定了技术基础。之后我国在《计算机信息系统安全保护等级划分准则》（GB17859—1999）的基础上进行了进一步的细化和扩展，相继出台了一系列的国家标准。2008年颁布的《信息系统安全等级保护基本要求》（GB/T 22239—2008）提出和规定了不同安全保护等级信息系统的最低技术和管理保护要求，将基本技术要求细分为信息安全类要求、服务保障类要求和通用安全保护类要求。《信息安全技术 信息系统安全等级保护定级指南》（GB/T 22240—2008）明确了信息安全的等级、定级要素、定级方法，并对定级要素的判定基准进行了细化。2010年发布的《信息安全技术 信息系统安全等级保护实施指南》（GB/T 25058—2010）提出了实施等级保护的四大基本原则：自主保护原则、重点保护原则、同步建设原则、动态调整原则。将信息系统安全等级保护实施的过程划分为信息系统定级阶段、总体安全规划、安全设计与实施、安全运行与维护、信息系统终止五个阶段，并规定了各阶段实施等级保护制度的要求。《信息安全技术 信息系统等级保护安全

设计技术要求》(GB/T 25070—2010)规定了信息系统等级保护安全设计技术要求,包括第一级至第五级系统安全保护环境的安全计算环境、安全区域边界、安全通信网络和安全管理中心等方面的设计技术要求,以及定级系统互联的设计技术要求。2012年发布的《信息安全技术 信息系统安全等级保护测评要求》(GB/T 28448—2012)、《信息安全技术 信息系统安全等级保护测评过程指南》(GB/T 28449—2012)对网络安全等级测评工作做出了细化规定。

## 二、网络安全等级保护制度 2.0 时代

进入新时期以来,中共中央办公厅、国务院办公厅《关于加强社会治安防控体系建设的意见》、《关于全面深化公安改革若干重大问题的框架意见》等文件中明确提出“健全网络安全等级保护制度”,《国家信息化发展战略纲要》、《国家网络空间安全战略》等战略中对等级保护工作提出了新要求,《网络安全法》从基本法层面确定了国家网络安全等级保护制度。以上文件法律的新要求标志着网络安全等级保护制度进入 2.0 时代,网络安全等级保护制度成为一个全新的国家网络安全基本制度体系,现阶段亟须进一步完善新的网络安全等级保护政策体系、标准规范体系、技术支撑体系、教育训练体系、等级测评体系和人才队伍体系等。

以标准规范体系为例,随着信息技术的迅速发展,云计算、大数据、物联网等新技术、新应用面临着更为复杂的网络安全环境,一些旧有的制度标准已经无法满足防护要求,原有的标准在适用性、时效性、易用性、可操作性等方面需要进一步完善。《网络安全法》出台以后,与网络安全等级保护制度配套的国家标准的制定和修订工作也在加紧推进中。全国信息标准委员会发布了一系列相关的征求意见稿。这些征求意见稿中的规定回应了时代和技术的要求。

这些征求意见稿大体可以分为两类:一类是对现有的标准进行修改和细化,例如,《信息安全技术 网络安全等级保护实施指南(征求意见稿)》即对《信息安全技术 信息系统安全等级保护实施指南》(GB/T 25058—2010)的修改和完善,《信息安全技术 网络安全等级保护基本要求 第 1 部分 安全通用要求(征求意见稿)》即对《信息系统安全等级保护基本要求》(GB/T 22239—2008)的修订。另一类是对网络安全等级保护 1.0 时代还没有关注、没有涉及的领域——云计算、

移动互联网、物联网、工业控制系统及大数据环境下的等级保护制度做出规定，例如，《信息安全技术 网络安全等级保护基本要求 第2部分：云计算安全扩展要求（征求意见稿）》、《信息安全技术 网络安全等级保护基本要求 第3部分：移动互联安全扩展要求（征求意见稿）》、《信息安全技术 网络安全等级保护基本要求 第4部分：物联网安全扩展要求（征求意见稿）》等。

### 三、网络安全等级保护实施的工作流程

网络安全等级保护工作实施的主要环节包括定级备案、建设整改、等级测评和监督检查。《信息安全等级保护管理办法》、《信息系统安全等级保护基本要求》、《信息系统安全等级保护实施指南》、《信息系统安全等级保护测评要求》、《信息系统安全等级保护测评过程指南》等规定和标准规定了各等级信息系统的保护措施，明确了对信息系统的定级、备案、测评、整改流程，以及安全管理要求和安全技术要求。

#### （一）定级备案

定级备案，即根据信息、信息系统的重要程度和信息系统遭到破坏后对国家安全、社会秩序、公共利益，以及公民、法人和其他组织的合法权益的危害程度，经公安机关审核把关，合理确定信息系统的安全保护等级。定级备案的主要依据是《信息安全等级保护管理办法》、《关于开展全国重要信息系统安全等级保护定级工作的通知》等规范性文件和《信息系统安全等级保护定级指南》等国家标准。一些行业主管部门依据上述文件和标准，结合行业实际，制定了更加具体的定级实施细则，用于指导全行业开展定级工作，这些实施细则可以作为该行业定级工作的依据。

定级备案环节包括了定级和备案两项工作。定级是指安全等级保护对象根据其在国家安全、经济建设、社会生活中的重要程度，遭到破坏后对国家安全、社会秩序、公共利益，以及公民、法人和其他组织的合法权益的危害程度等确定安全保护等级。影响定级的两个影响因素为重要程度和危害程度。其中危害程度考量的因素为公民、法人和其他组织的合法权益，社会秩序、公共利益，以及国家

安全。依据上述因素,《信息安全技术 信息系统安全等级保护定级指南》(GB/T 22240—2008)将安全保护等级由低到高划分为五个等级。定级要素与安全保护等级的关系如表 5-1 所示。

表 5-1 安全保护等级的关系

受侵害的客体	对客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第二级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

需要注意的是《信息安全技术 网络安全等级保护基本要求 第 1 部分:安全通用要求(征求意见稿)》对 GB/T 22240—2008 做了一定的修改。根据后者的规定,遭到破坏后会对公民、法人和其他组织的合法权益造成损害的安全等级保护对象的安全保护等级最高为第二级,但《信息安全技术 网络安全等级保护基本要求 第 1 部分:安全通用要求(征求意见稿)》将遭到破坏后会对公民、法人和其他组织的合法权益造成特别严重损害的安全等级保护对象的安全保护等级规定为第三级。

定级是等级保护工作的首要环节和关键环节,是开展系统备案、建设整改、等级测评和监督检查等工作的重要基础。系统安全级别定级不准,系统备案、建设整改、等级测评等后续工作会失去基础,需做到科学、合理、准确定级。实践中,在定级对象和保护等级的选取上需注意以下内容:第一,起支撑、传输作用的基础网络(包括专网、内网、外网、网管系统)是定级对象,可从安全管理和安全责任角度将基础网络划分为若干安全域定级;第二,用于生产、调度、管理、作业、指挥、办公等目的的各类业务应用系统,按照不同业务类别单独确定为定级对象;第三,单位、部门的门户网站,以及对外提供信息发布、内容服务的政务公开平台等应作为独立的定级对象;第四,对于云平台、大数据、工业控制系统、物联网、移动互联网、卫星系统等,要合理确定定级对象,科学确定保护等级。

网络运营者完成定级后,还应当根据有关规定进行备案。根据公安部 2007 年发布的《信息安全等级保护备案实施细则》(公信安[2007]1360 号)的规定,公安机关公共信息网络安全监察部门为定级工作的备案单位。信息系统运营、

使用单位或其主管部门应当在信息系统安全保护等级确定后 30 日内，到公安机关公共信息网络安全监察部门办理备案手续。《信息安全等级保护管理办法》规定信息系统运营、使用单位应当根据已经确定的安全保护等级，到公安机关办理备案手续；《信息安全技术 网络安全等级保护基本要求 第 1 部分：安全通用要求（征求意见稿）》也规定了网络运营者的网络安全保护等级定级工作完成后，运营、使用单位有主管部门的，应当经主管部门审核、批准，并报公安机关备案审查。

## （二）建设整改

系统安全保护等级确定后，网络运营者根据信息系统的安全级别为信息系统选择最低安全控制措施，并在信息系统中实现这些安全技术措施和管理措施，确保信息系统具有与其安全级别对应的安全保护能力，建设整改工作是网络安全等级保护制度的核心和落脚点。

建设整改的主要依据是《关于开展信息系统等级保护安全建设整改工作的指导意见》（公信安〔2009〕1429 号）、《信息安全等级保护安全建设整改工作指南》等规范性文件和《信息系统安全等级保护基本要求》、《信息系统安全管理要求》、《信息系统安全等级保护实施指南》、《信息系统安全工程管理要求》、《信息系统通用安全技术要求》、《信息系统等级保护安全设计技术要求》等国家标准。

## （三）等级测评

等级测评是等级保护工作的重要环节，网络运营者通过委托等级测评机构开展等级测评，可以查找系统安全隐患和薄弱环节，明确系统与相应等级标准要求的差距和不足，有针对性地进行安全建设整改。等级测评机构是指具备《信息安全等级保护测评工作管理规范》确定的基本条件，经能力评估和审核，由省级以上信息安全等级保护工作协调（领导）小组办公室推荐，从事等级测评工作的机构。等级测评作为特殊的安全服务，对于检验网络运营者安全保护措施落实情况，促进其不断优化和改进安全保护状况，提升我国网络安全总体防护水平具有十分重要的意义。2010 年，公安部在 2009 年试点工作基础上，正式开展测评机构推

荐工作。截至 2016 年年底，全国共审核推荐了 156 家等级测评机构。

等级测评的主要依据是《信息安全等级保护管理办法》、《关于加强国家电子政务工程建设项目信息安全风险评估工作的通知》（发改高技〔2008〕2071 号）、《关于推动信息安全等级保护测评体系建设和开展等级测评工作的通知》（公信安〔2010〕303 号），附件包含《信息安全等级保护测评工作管理规范》、《关于印发〈信息系统安全等级测评报告模版（试行）〉的通知》（公信安〔2009〕1487 号）等规范性文件和《信息系统安全等级保护测评要求》、《信息系统安全等级保护测评过程指南》等国家标准。

#### （四）监督检查

为规范公安机关开展等级保护检查工作，公安部十一局根据《信息安全等级保护管理办法》制定了《公安机关信息安全等级保护检查工作规范（试行）》，会同主管部门对非涉密重要信息系统运营使用单位等级保护工作开展和落实情况进行检查，对第三级信息系统的运营使用单位信息安全等级保护工作每年检查一次，对第四级信息系统的运营使用单位信息安全等级保护工作每半年检查一次，确保网络安全等级保护工作落到实处。公安机关检查内容包括等级保护工作部署和组织情况、信息系统安全等级保护定级备案情况、信息安全设施建设情况和信息安全整改情况、信息安全管理制度的建立和落实情况、信息安全产品选择和使用情况、聘请测评机构开展技术测评工作情况、定期自查情况等。

### 第三节 网络安全等级保护法规遵从框架及建议

我国对于网络安全等级保护的规定最早出现在 20 世纪 90 年代，主要表现为保障计算机信息系统安全。近年来随着新一代信息技术的发展、共享经济的兴起，我国在这些关键领域对于等级保护制度也做出相应要求。表 5-2 中所列法律、政策文件、指导意见和规范初步构成了我国信息安全等级保护政策体系，为指导等级保护工作提供了保障。

表 5-2 网络安全等级保护的法规遵从框架

法律名称	法律条款	法律规定
1994《计算机信息系统安全保护条例》(国务院令 147 号)	第九条	计算机信息系统实行安全等级保护, 安全等级的划分标准和安全等级保护的具体办法由公安部会同有关部门制定
2003《国家信息化领导小组关于加强信息安全保障工作的意见》	(二)	要重点保护基础信息网络和关系国家安全、经济命脉、社会稳定等方面的重要信息系统, 抓紧建立信息安全等级保护制度, 制定信息安全等级保护的管理办法和技术指南
2004《关于信息安全等级保护工作的实施意见》(公通字[2004] 66 号)	全文	主要包括贯彻落实信息安全等级保护制度的基本原则, 等级保护工作的基本内容、工作要求和实施计划, 以及各部门工作职责分工等
2007《信息安全等级保护管理办法》(公通字[2007] 43 号)	全文	明确公安部牵头, 会同国家保密局、国家密码管理局等部门共同组织实施信息安全等级保护工作, 同时明确了中国的信息安全等级保护工作包括定级备案、建设整改、等级测评和监督检查几个环节
2007《关于开展全国重要信息系统安全等级保护定级工作的通知》(公通字[2007] 861 号)	全文	明确定级范围、定级工作的主要内容及要求, 标志着全国范围内信息安全等级保护定级工作的开展
2007《信息安全等级保护备案实施细则》(公信安[2007] 1360 号)	全文	本细则适用于非涉及国家秘密的第二级以上信息系统的备案
2008《公安机关信息安全等级保护检查工作规范》(公信安[2008] 736 号)	全文	本规范旨在规范公安机关公共信息网络安全监察部门开展的信息安全等级保护检查工作
2008《关于加强国家电子政务工程建设项目信息安全风险评估工作的通知》(发改高技[2008] 2071 号)	全文	通知适用于电子政务项目(国家的电子政务网络、重点业务信息系统、基础信息库及相关支撑体系等国家电子政务工程建设项目)开展信息安全风险评估工作
2009《关于开展信息系统等级保护安全建设整改工作的指导意见》(公信安[2009] 1429 号)	全文	明确整改工作的目标、细化工作内容、落实工作要求, 标志着全国范围内信息安全等级保护建设整改工作的启动
2009《关于印发〈信息系统安全等级测评报告模版(试行)〉的通知》(公信安[2009] 1487 号)	全文	通知内容旨在规范等级测评活动并按照统一的格式编制测评报告

续表

法律名称	法律条款	法律规定
2009《电子文件管理暂行办法》	第二十条	<p>电子文件保管应当符合下列要求：</p> <p>（一）按照国家信息安全等级保护标准和涉密信息系统分级保护管理规定建立电子文件管理系统和信息内容安全保密防护体系，执行严格的安全保密管理制度；</p> <p>（二）定期对电子文件的保管情况、可读取状况等进行测试、检查，发现问题及时处理；</p> <p>（三）电子文件运行的软硬件环境、存储载体等发生变化时，应当将其及时迁移、转换；</p> <p>（四）电子文件应当实行备份制度；</p> <p>（五）根据电子文件不同载体保管环境的要求，选择适宜的保管条件</p>
2010《关于推动信息安全等级保护测评体系建设和开展等级测评工作的通知》（公信安〔2010〕303号）	全文	通知明确工作目标、内容和要求，标志着全国范围内信息安全等级保护测评工作的开始
2010《关于做好信息安全等级保护测评机构审核推荐工作的通知》（公信安〔2010〕559号）	全文	明确等级测评机构审核推荐工作流程和方法
2010《关于进一步推进中央企业信息安全等级保护工作的通知》（公通字〔2010〕70号）	全文	<p>通知明确应切实将信息安全等级保护工作纳入企业信息化工作同步推进；建立分工负责、协作配合的工作机制；全面梳理企业信息网络和系统，认真做好企业信息系统安全等级保护定级、备案工作；开展信息安全等级保护安全建设整改和等级测评工作，完善重要信息系统安全防护体系；加强检查和考核，确保信息系统安全保护能力达到等级保护要求</p>
2014《电力监控系统安全防护规定》	第二条	<p>电力监控系统安全防护工作应当落实国家信息安全等级保护制度，按照国家信息安全等级保护的有关要求，坚持“安全分区、网络专用、横向隔离、纵向认证”的原则，保障电力监控系统的安全</p>
2016《网络借贷信息中介机构业务活动管理暂行办法》	第十八条	<p>网络借贷信息中介机构应当按照国家网络安全相关法规和国家信息安全等级保护制度的要求，开展信息系统定级备案和等级测试，具有完善的防火墙、入侵检测、数据加密，以及灾难恢复等网络安全设施和管理制度，建立信息科技管理、科技风险管理和科技审计有关制度，配置充足的资源，采取完善的管理控制措施和技术手段保障信息系统安全稳健运行，保护出借人与借款人的信息安全</p>



续表

法律名称	法律条款	法律规定
2016《网络安全法》	第二十一条	<p>国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或未经授权的访问，防止网络数据泄露或者被窃取、篡改：</p> <p>（一）制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；</p> <p>（二）采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施；</p> <p>（三）采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于 6 个月；</p> <p>（四）采取数据分类、重要数据备份和加密等措施；</p> <p>（五）法律、行政法规规定的其他义务</p>
	第五十九条	<p>网络运营者不履行本法第二十一条、第二十五条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或导致危害网络安全等后果的，处一万元以上十万元以下罚款，对直接负责的主管人员处五千元以上五万元以下罚款。</p> <p>关键信息基础设施的运营者不履行本法第三十三条、第三十四条、第三十六条、第三十八条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款</p>
2016《全国测绘地理信息应用成果和地图上展览运行维护管理办法》	第七条	各地、各有关单位应制定展馆运维应急预案、建立展馆运维保障机制、加强安全技术防护措施。各展馆运维负责人应定期登录展览系统、发布平台和相应展馆，检定运行状况、核查展示内容、排除技术漏洞和安全隐患。各展馆安全防护措施应当符合国家信息安全等级保护二级要求
2017《公安信息网安全管理规定（试行）》	第九条	公安信息网及其网上的应用系统应当执行国家网络安全等级保护管理制度，开展定级备案、等级测评、安全建设等工作
2017《全国投资项目在线审批监管平台运行管理暂行办法》	第二十一条	各级在线平台要满足国家信息安全等级保护第三级的有关要求。建设运维部门要实时监控在线平台运行情况，严格实行安全防护策略，完善数据备份、恢复和容灾机制
2017《国家企业信用信息公示系统使用运行管理办法（试行）》	第二十二条	工商总局及省级工商部门应当按照信息系统安全等级保护基本要求（GB/T 22239—2008）中关于第三级信息系统的技术和管理要求，建立公示系统安全管理制度，落实安全保障措施，加强日常运行监控，做好安全防护

作为法律遵从的重要主体之一，网络运营者高效正确地将法律规定落到实处，将着力提升法律本身的价值。当前我国对于网络安全等级保护制度公布了一系列规定，表 5-3 主要依据《信息安全技术 网络安全等级保护实施指南（征求意见稿）》，按照等级保护的操作流程将遵从分为网络安全等级的定级备案、总体规划、安全设计与实施、安全运行与维护、应急响应与保障、定级对象的终止六部分，列明网络运营者应采取的具体措施，从而为网络运营者提供指引。

表 5-3 网络安全等级保护的法规遵从建议

控制项	网络安全等级保护的法规遵从建议	对应条款
1. 网络安全等级的定级备案		第二十一条
行业/领域定级工作	行业/领域主管部门在必要时可组织梳理行业/领域的主要社会功能/职能及作用，分析主要社会功能/职能的履行依赖的主要业务及服务范围，最后依据分析和整理的内容形成行业/领域的业务总体描述性文档	国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或未经授权的访问，防止网络数据泄露或者被窃取、篡改：
等级保护对象分析	<p>组织应通过收集了解有关等级保护对象的信息，并对信息进行综合分析和整理，分析组织的主要社会功能/职能及作用，确定主要社会功能/职能的履行依赖的等级保护对象，整理等级保护对象处理的业务及服务范围，最后依据分析和整理的内容，有行业/领域定级指导意见的还应依据行业/领域定级指导意见，形成组织内等级保护对象的总体描述性文档。</p> <p>组织应依据单位的等级保护对象总体描述文件（有行业/领域定级指导意见的还应依据行业/领域定级指导意见），在综合分析的基础上将组织内运行的等级保护对象进行合理分解，确定所包含的定级对象及其个数</p>	（一）制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；
安全保护等级确定	<p>组织应按照国家有关管理规范 and GB/T 22240，确定定级对象的安全保护等级，并对定级结果进行评审、审核和审查，保证定级结果的准确性。</p> <p>组织应对定级过程中产生的文档进行整理，形成等级保护对象定级结果报告</p>	（二）采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施；
定级结果备案	组织应根据国家管理部门对备案的要求，整理相关备案材料，并向受理备案的单位提交备案材料	（三）采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；
2. 网络安全等级保护的总体规划		（四）采取数据分类、重要数据备份和加密等措施；
规划的安全需求分析	组织应根据等级保护对象的安全保护等级，提出等级保护对象的基本安全保护需求。	（五）法律、行政法规规定的其他义务

续表

控制项	网络安全等级保护的法规遵从建议	对应条款
规划的安全需求分析	<p>组织应通过对等级保护对象重要资产特殊保护要求的分析，确定超出相应等级保护基本要求系列标准和行业基本要求的部分或具有特殊安全保护要求的部分，采用需求分析或风险分析的方法，确定可能的安全风险，判断对超出等级保护基本要求系列标准和行业基本要求的部分实施特殊安全措施必要性，提出等级保护对象的特殊安全保护需求。</p> <p>组织应总结基本安全需求和特殊安全需求，形成安全需求分析报告</p>	
规划的总体安全设计	<p>组织应形成机构纲领性的安全策略文件，包括确定安全方针，制定安全策略，以便结合等级保护基本要求系列标准、行业基本要求和安全保护特殊要求，构建机构等级保护对象的安全技术体系结构和安全管理体系结构。对于新建的等级保护对象，应在立项时明确其安全保护等级，并按照相应的保护等级要求进行总体安全策略设计。</p> <p>组织应根据 GB/T 22239、行业基本要求、安全需求分析报告、机构总体安全策略文件等，提出等级保护对象需要实现的安全技术措施，形成机构特定的等级保护对象安全技术体系结构，用以指导等级保护对象分等级保护的具体实现。</p> <p>组织应根据等级保护基本要求系列标准、行业基本要求、安全需求分析报告、机构总体安全策略文件等，调整原有管理模式和管理策略，既从全局高度考虑为每个等级的定级对象制定统一的安全管理策略，又从每个定级对象的实际需求出发，选择和调整具体的安全管理措施，最后形成统一的整体安全管理体系结构。</p> <p>组织应将总体安全设计工作的结果文档化，最后形成一套指导机构信息安全工作的指导性文件</p>	
安全建设项目规划	<p>组织应依据等级保护对象安全总体方案（一个或多个文件构成）、组织信息化建设的中长期发展规划和机构的安全建设资金状况确定各时期的安全建设目标。</p> <p>组织应根据安全建设目标和等级保护对象安全总体方案的要求，设计分期分批的主要建设内容，并将建设内容组合成不同的项目，阐明项目之间的依赖或促进关系等。</p> <p>组织应根据建设目标和建设内容，在时间和经费上对安全建设项目列表进行总体考虑，分到不同的时期和阶段，设计建设顺序，进行投资估算，形成安全建设项目规划</p>	

续表

控制项	网络安全等级保护的法规遵从建议	对应条款
3. 网络安全等级保护的安全设计与实施		
安全方案的详细设计要求	<p>技术措施方面，组织应根据建设目标和建设内容将等级保护对象安全总体方案中要求实现的安全策略、安全技术体系结构、安全措施和要求落实到产品功能或物理形态上，提出能够实现的产品或组件及其具体规范，并将产品功能特征整理成文档，使得在信息安全产品采购和安全控制开发阶段具有依据。</p> <p>管理措施方面，组织应根据等级保护对象运营、使用单位当前安全管理需要和安全技术保障需要提出与等级保护对象安全总体方案中管理部分相适应的本期安全实施内容，以保证在安全技术建设的同时，安全管理得以同步建设。</p> <p>组织应将技术措施实施方案、管理措施实施方案汇总，同时考虑工时和成本，最后形成指导安全实施的指导性文件</p>	
技术措施的实现要求	<p>组织应按照安全详细设计方案中对于产品或服务的具体指标要求进行采购，根据产品、产品组合或服务实现的功能、性能和安全性满足安全设计要求的情况来选购所需的信息安全产品或服务。</p> <p>组织对于一些不能通过采购现有信息安全产品来实现的安全措施和安全功能，通过专门进行的设计、开发来实现。安全控制的开发应当与系统的应用开发同步设计、同步实施，而应用系统一旦开发完成后，再增加安全措施会造成很大的成本投入。因此，在应用系统开发的同时，要依据安全详细设计方案进行安全控制的开发设计，保证系统应用与安全控制同步建设。</p> <p>组织应将不同的软硬件产品进行集成，依据安全详细设计方案，将信息安全产品、系统软件平台和开发的安全控制模块与各种应用系统综合、整合成为一个系统。安全控制集成的过程可以运营、使用单位与信息安全服务机构共同参与、相互配合，把安全实施、风险控制、质量控制等有机结合起来，实现安全态势感知、监测通报预警、应急处置追踪溯源等安全措施，构建统一安全管理平台。</p> <p>组织应检验系统是否严格按照安全详细设计方案进行建设，是否实现了设计的功能、性能和安全性。在安全控制集成工作完成后，系统测试及验收是从总体出发，对整个系统进行集成性安全测试，包括对系统运行效率和可靠性的测试，也包括管理措施落实内容的验收</p>	

续表

控制项	网络安全等级保护的法规遵从建议	对应条款
管 理 措 施 的实现要求	<p>组织应依据国家信息安全相关政策、标准、规范，制定、修订并落实与等级保护对象安全管理相配套的、包括等级保护对象的建设、开发、运行、维护、升级和改造等各阶段和环节所应当遵循的行为规范和操作规程。</p> <p>组织应建立配套的安全管理职能部门，通过管理机构的岗位设置、人员的分工和岗位培训及各种资源的配备，保证人员具有与其岗位职责相适应的技术能力和管理能力，为等级保护对象的安全管理提供组织上的保障。</p> <p>组织应在等级保护对象定级、规划设计、实施过程中，对工程的质量、进度、文档和变更等方面的工作进行监督控制和科学管理</p>	
4. 网络安全等级保护的安全运行与维护		
运行的管理 和控制要求	<p>组织应通过对运行管理活动或任务的角色划分，并授予相应的管理权限，来确定安全运行管理的具体人员和职责。应至少划分为系统管理员、安全管理员及安全审计员。</p> <p>组织应通过制定运行管理操作规程，确定运行管理人员的操作目的、操作内容、操作时间和地点、操作方法和流程等，并进行操作过程记录，确保对操作过程进行控制</p>	
变更的管理 和控制要求	<p>组织应通过对运行与维护过程中的变更需求和变更影响的分析，来确定变更的类别，计划后续的活动内容。</p> <p>组织应确保运行与维护过程中的变更实施过程受到控制，各项变化内容进行记录，保证变更对业务的影响最小</p>	
安 全 状 态 的监控要求	<p>组织应确定可能对等级保护对象安全造成影响的因素，即确定安全状态监控的对象。</p> <p>组织应选择状态监控工具，收集安全状态监控的信息，识别和记录入侵行为，对等级保护对象的安全状态进行监控。</p> <p>组织应通过对安全状态信息进行分析，及时发现安全事件或安全变更需求，并对其影响程度和范围进行分析，形成安全状态结果分析报告</p>	
安 全 自 查 和持续改进	<p>组织应通过对等级保护对象的安全状态进行自查，为等级保护对象的持续改进过程提供依据和建议，确保等级保护对象的安全保护能力满足相应等级安全要求。</p> <p>组织应依据安全检查的结果，调整等级保护对象的安全状态，保证等级保护对象安全防护的有效性。</p> <p>组织应保证按照安全改进方案实现各项补充安全措施，并确保原有的技术措施和管理措施与各项补充的安全措施一致有效地工作</p>	

续表

控制项	网络安全等级保护的法规遵从建议	对应条款
服务商管理和监控要求	<p>组织在选择服务商时，应确定其符合国家规定或行业规定的设计、测评、建设资质。</p> <p>组织应对服务商从多维度进行切实有效管理，使得服务商在约定范围内开展服务工作。</p> <p>组织应对服务商及其人员在服务过程中的行为进行有效监控，若发现不合规行为，限时保质整改</p>	
等级测评要求	信息安全等级测评机构依据有关等级保护对象安全保护等级测评的规范或标准对等级保护对象开展等级测评；组织应参考等级测评出具的安全等级测评报告，分析确定整改需求	
监督检查要求	国家管理部门、主管部门依据国家信息安全等级保护、行业监管要求等制定监督检查方案及表格；组织应根据信息安全保护等级保护监督检查、行业监管的规范或标准，准备相应的监督检查所需材料	
5. 网络安全等级保护的应急响应与保障		
应急准备与预案要求	<p>组织应建立完善的应急组织体系，并且通过分析安全事件的等级，在统一的应急预案框架下制定不同安全事件的应急预案。</p> <p>组织应明确应急预案演练的规模、方式、范围、内容、组织、评估、总结等内容，并按照预案定期开展演练</p>	
应急监测与响应要求	<p>组织应收集异常安全状态监控的信息，识别和记录入侵行为，对等级保护对象的安全状态进行监控，并根据应急预案启动条件研判是否启动应急程序。</p> <p>组织应对监控到的安全事件采取适当的方法进行预处置，对安全事件的影响程度和等级进行分析，确定应启动相应级别的应急预案。</p> <p>组织应对安全事件的影响程度和等级分析情况，启动相应级别的应急预案，按照应急预案流程，开展应急响应处置工作</p>	
后期评估与改进要求	组织应对安全事件原因、处置过程进行调查分析，并根据分析结果进行责任认定及制定改进预防措施	
应急保障要求	组织应建立健全应急保障体系，针对各类专项应急预案进行分析，制定应急预案执行所需通信、装备、数据、队伍、交通运输、经费及治安保障内容	
6. 网络安全等级保护定级对象的终止		
信息转移、暂存和消除要求	组织应在等级保护对象终止处理过程中，对于可能在另外的等级保护对象中使用的信息采取适当的方法将其安全地转移或暂存到可以恢复的介质中，确保将来可以继续使用，同时采用安全的方法清除要终止的等级保护对象中的信息	

续表

控制项	网络安全等级保护的法规遵从建议	对应条款
设备迁移或废弃要求	组织应确保等级保护对象终止后，迁移或废弃的设备内不包括敏感信息，对设备的处理方式应符合国家相关部门的要求	
存储介质的消除或销毁要求	组织应通过采用合理的方式对计算机介质（包括磁带、磁盘、打印结果和文档）进行信息清除或销毁处理，防止介质内的敏感信息泄露	

第四节 监督管理与法律责任

一、监督管理

《网络安全法》第八条确定了我国网络安全整体的监督管理体制，即国家网信部门负责统筹协调网络安全工作和相关监督管理工作。国务院电信主管部门、公安部门和其他有关机关依照本法和有关法律、行政法规的规定，在各自职责范围内负责网络安全保护和监督管理工作。县级以上地方人民政府有关部门的网络安全保护和监督管理职责，按照国家有关规定确定。

在“有关法律、行政法规的规定”上，1994 年国务院第 147 号令《计算机信息系统安全保护条例》第九条明确“计算机信息系统实行安全等级保护，安全等级的划分标准和安全等级保护的具体办法，由公安部会同有关部门制定”，首次以国家行政法规形式确立了信息安全等级保护制度的法律地位。2003 年中国共产党中央委员会办公厅（以下简称“中办”）、中华人民共和国国务院办公厅（以下简称“国办”）转发的《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发〔2003〕27 号）中明确提出“实行信息安全等级保护”，“要重点保护基础信息网络和关系国家安全、经济命脉、社会稳定等方面的重要信息系统，抓紧建立信息安全等级保护制度，制定信息安全等级保护的管理办法和技术指南”等意见。2003 年 8 月，在上届国家网络与信息安全协调小组办公室制定的贯彻落实 27 号文件的工作安排中，明确将实行信息安全等级保护工作交由公安部牵头，并要求公安部会同有关部门研究提出实行信息安全等级保护的意見。2004 年 7 月召开的

国家网络与信息安全协调小组第三次会议上，原则同意了公安部提出的《关于信息安全等级保护工作的实施意见》，责成公安部商有关部门联合印发。2004 年 9 月 15 日，公安部、国家保密局、国家密码管理委员会、国务院信息化工作办公室向各地有关部门联合下发了《关于印发〈关于信息安全等级保护工作的实施意见〉的通知》（公通字〔2004〕66 号）。在 2008 年国务院“三定”方案中，进一步规定了公安部十一局监督、检查、指导信息安全等级保护工作的职能。

这些法规和政策性文件的制定，确立了信息安全等级保护制度的法律地位，明确了实行信息安全等级保护是我国信息安全保障工作中一项重要制度和措施，赋予了公安机关牵头负责信息安全等级保护工作监督管理的职责。因此，公安机关将依据《网络安全法》、《人民警察法》、《计算机信息系统安全保护条例》等法律、行政法规的规定，负责等级保护的监督管理，继续实施等级保护工作部署和组织情况、信息系统安全等级保护定级备案情况、信息安全设施建设情况和信息安全整改情况、信息安全管理制度建立和落实情况、信息安全产品选择和使用情况、聘请测评机构开展技术测评工作情况、定期自查情况等具体工作。

总体来说，《网络安全法》确立了国家网信部门统筹协调，电信主管部门、公安部门等在各自职责范围内负责的管理体制，使得在包括网络安全等级保护等制度设计的落实层面应注意协调现有主管部门和整体管理体制之间的关系，充分发挥已有管理经验和行政资源，科学管理，提高行政效率。

## 二、法律责任

违反网络安全等级保护责任的法律责任主要体现为《网络安全法》第五十九条，即网络运营者不履行本法第二十一条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或导致危害网络安全等后果的，处一万元以上十万元以下罚款，对直接负责的主管人员处五千元以上五万元以下罚款。

由此可见，承担网络安全等级保护责任的主体不仅包括网络运营者，还包括直接负责的主管人员，处罚方式包括责令改正后警告和罚款。其中责令改正警告属于未造成危害后果的前置条件，拒不改正后进一步做出罚款处罚；在网络运营者不履行安全保护义务导致危害网络安全后果的情形下，可直接做出罚款处罚。



《网络安全法》实施之后，网络安全执法行为逐渐走向常态。从目前的执法情况来看，部分属于违反网络安全等级制度的处罚案例，这在一定程度上反映了《网络安全法》中规定的网络安全等级制度在实践中尚未得到很好的贯彻和落实。案例中违反网络安全等级保护的行为，包括未按规定进行网络安全等级的定级备案与等级测评、未留存网络日志、未对危害网络安全的行为采取技术防范措施等。具体的执法案例如表 5-4 所示。

表 5-4 网络安全等级保护制度执法案例汇总

事件	执法机关	处罚行为	处罚措施
汕头某公司违反《网络安全法》被查处	广东汕头网警支队	未按规定履行网络安全等级测评义务	警告、责令改正
重庆某网络公司违反《网络安全法》被查处	重庆公安局网安总队	未依法留存用户登录相关网络日志	警告、责令改正
四川某教育网站违反《网络安全法》被查处	宜宾网安部门	未进行网络安全等级保护的定级备案、等级测评等工作，未落实网络安全等级保护制度	对直接负责的主管人员罚款五千元，机构罚款一万元
山西某网站违反《网络安全法》被查处	山西忻州市、县两级公安机关网安部门	未采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施	警告、责令改正
安徽网警依法查处一起违反网络安全等级保护制度案件	安徽省公安厅网络安全保卫总队、蚌埠市局网安支队	未进行网络安全等级保护的定级备案、等级测评等工作	对学校罚款一万五千元，对直接负责人罚款五千元

# 实名制与可信身份战略

## 第一节 《网络安全法》相关规定及释义

《网络安全法》第二十四条明确规定，网络运营者为用户办理网络接入、域名注册服务，办理固定电话、移动电话等入网手续，或者为用户提供信息发布、即时通信等服务，在与用户签订协议或确认提供服务时，应当要求用户提供真实身份信息。用户不提供真实身份信息的，网络运营者不得为其提供相关服务。国家实施网络可信身份战略，支持研究开发安全、方便的电子身份认证技术，推动不同电子身份认证之间的互认。

按照《网络安全法》界定，网络实名制是指网络运营商提供限定范围内的网络服务时应当要求用户提供真实身份信息的制度，主要涉及入网服务、发布信息和即时通信服务。相比较之前实名制的规定，此次《网络安全法》第二十四条的规定是较为全面的一次规定，实用范围比之前的相关规定广。

网络运营商是指网络所有者、管理者和网络服务提供者，网络服务提供商和网络内容提供商、网站、个人网页、网络电子公告服务等都属于实名制实施的规范范畴。这里网络管理者主要是指网络操作系统、网络数据库、网络设备、网络管理、网络安全、应用开发等方面的实施管理的运营主体。

网络服务提供者主要是指包括为广大网络用户提供多媒体互联网在线网络服务的经营主体的统称。

网络接入服务提供商所使用的硬件设施在用户实现联网功能后仅仅起到“传输通道”的作用，并且服务商不能对传输的信息内容进行控制。常见的该类服务的提供商有中国联通、中国电信及电视公司所提供的一系列上网业务。

身份信息：按照法律规定，作为网络所有者，在提供接入服务时应要求用户提供真实身份信息。实践中，基本上网络所有者在提供网络接入服务时均会要求接入服务者提供真实身份信息，即通常的身份信息。例如，在办理固定电话、移动电话等入网手续时服务商对证件严格核验并复印登记，并确保所用手机号码都与身份真实的个人一一对应。

域名注册服务：域名是互联网上企业或机构的标识，是互联网上各网站间相互联系的地址，由一串用点分隔的名字组成。基于解决地址对应问题，域名需要注册获得，且每个域名都是独一无二的，而且遵循先注册原则。域名注册的主体可以为企业也可以为个人，基于域名的标识性，域名注册服务实名制的实施可以准确定位其注册者，从而确保监管的有效性，以及网站的安全性。

为用户提供信息发布：主要是指网络内容服务提供，包括网络用户开立博客、论坛发帖等不同类型的信息发布。由于网络中间服务商的网络基础设施经营者和网络接入服务提供者对网上信息也完全不具有控制能力，其主要为各种在线业务提供线缆、路由器、交换机等基础通信服务，或者提供客户机与服务器的连接服务。

目前，当平台运营商为用户提供信息发布服务时，匿名信息发布机制下服务提供商主要提供网络空间服务如个人主页、网络硬盘、下载信息，提供上传、存储、发布信息内容服务，为避免因提供信息发布服务而导致的网络信息安全问题，在实名制实施下，需要进行实名身份认证，以杜绝不良信息及其盗版作品在网络上传播。

## 第二节 网络实名制与可信身份战略制度概述

### 一、国外制度概述

#### （一）美国《网络空间可信身份战略》

美国没有强制的立法推进网络实名制，但其重视网络环境下可信身份制度的

建构。2010年6月25日，美国发布了《网络空间中可信身份的国家战略》(National Strategy for Trusted Identities in Cyberspace, NSTIC)，该战略旨在建立综合的网络身份管理系统，以此推出网络身份证，同时重点关注公民隐私保护、安全保障和使用便利等具体问题。美国希望通过该战略的实施，建立一个安全环境，在这个环境里，个人用户可以自行选择认证服务提供者(或私或公)，以获得一个安全的、共用的、可加强隐私保护的身份证明(如智能卡、手机的数字证书等)，来保证各种在线业务(如网上银行、医疗保健记录、发送电子邮件等)的身份认证安全。该战略提出了四个基本指导原则：一是安全可靠、二是互通共用、三是隐私保护和自由选择、四是成本效益和易于使用。

美国可信身份系统的建构基于安全、隐私、可信和便利宗旨，主要由私有机构和企业实际参与和推进，政府部门负责提供相应技术标准支持，用户自愿选择和自由参与使用网络身份证。

## (二) 欧盟网络身份管理政策法规

欧盟倡导推行欧洲数字议程，发布有“i2010 战略计划”、“欧洲电子政务行动计划 2011—2015”、“欧洲 2020 战略计划”。为推行其数字议程电子政务计划，提供跨界的公共服务，欧盟推行实施网络身份认证和管理计划，并注重立法保障网络身份管理计划的实施；重视相应技术，尤其是互操作性技术的创新和研发；重视支撑网络身份管理实施的标准化建设，以及该技术推进中的用户信息安全保障。

为保障网络电子身份证计划的实施和推进，欧盟委员会对欧盟及其成员推行电子身份管理进行了统筹规划。2006年欧盟委员会发布了《2010 泛欧洲电子身份管理框架路线图》，2009年欧盟发布电子身份管理行动的报告(Report on the state of pan-European eIDM initiatives, 2009)，重视电子身份的管理，提出欧洲电子身份证的管理倡议，倡议内容要求提高跨境身份证明和跨境身份证资源的可用性。欧盟规范并推动电子身份证在欧盟范围内推广应用，不断细化电子身份证跨境应用的规则和操作规范。2014年颁布了《内部市场电子交易电子签名和信任服务规则》，以实现在电子签名，电子文件传输、网站认证、时间戳等方面可信服务市场的构建。

为规范电子身份的管理,确保欧盟成员可以使用其自己国家的电子身份证访问他国的公共服务,欧盟重视网络跨境可信应用和互操作性标准制定,已制定的标准涉及可信服务(包括支持电子签名的时间戳服务、证书服务、签名生成和验证服务标准等)和可信应用服务(包括应用电子签名的注册电子邮件、数据保存、电子发票标准等),以及可信服务状态列表(包括可信服务状态、可信服务提供商状态列表等)等相关标准。而统一的技术标准是解决网络身份管理互通互认的重要基础和支撑,显然欧盟在此方面已经提供了很好的借鉴。

## 二、我国实名身份管理制度的意义

对于实名身份管理在构建可信的网络空间环境方面的意义,可信网络空间构建对实名身份管理的需求主要包括以下两个方面:在政府服务方面,为电子政务服务、公众安全服务、国家安全服务等方面提供身份保证服务和能力;在商业应用方面,通过使用通用的身份管理基础设施提供身份保证功能与能力,实现各种应用和业务的连接。这些新的要求使互联网身份管理将面临新的挑战,需要构建综合的互联网电子身份管理及完善相应的法律制度。

任何一个国家构建网络空间可信身份制度需应对的挑战包括政治、法律、隐私问题、预算、采购机制、组织协调模式、技术、高层支持与治理、数据可用性与可访问性安全问题等<sup>①</sup>。

## 第三节 网络实名制的法规遵从框架及建议

### 一、网络实名制的法规遵从框架

除了《网络安全法》之外,我国还有其他部门法和地方规章制度对关键信息基础设施的运营者采购网络产品和服务时的保密义务与责任有所规定(见表6-1)。

---

<sup>①</sup> 黄道丽. 国家网络空间可信身份制度研究——以英国电子身份管理(eIDM)制度为个案[R/OL]. [2006]. [www.cnki.com.cn](http://www.cnki.com.cn).

表 6-1 网络实名制的法规遵从框架

法律名称	法律条款	法律规定
《网络安全法》	第二十四条	网络运营者为用户办理网络接入、域名注册服务，办理固定电话、移动电话等入网手续，或者为用户提供信息发布、即时通信等服务，在与用户签订协议或确认提供服务时，应当要求用户提供真实身份信息。用户不提供真实身份信息的，网络运营者不得为其提供相关服务。国家实施网络可信身份战略，支持研究开发安全、方便的电子身份认证技术，推动不同电子身份认证之间的互认
	第六十一条	网络运营者违反本法第二十四条第一款规定，未要求用户提供真实身份信息，或者对不提供真实身份信息的用户提供相关服务的，由有关主管部门责令改正；拒不改正或情节严重的，处五万元以上五十万元以下罚款，并可以由有关主管部门责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款
	第七十六条	本法下列用语的含义：（五）个人信息，是指以电子或其他方式记录的能够单独或与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等
《中华人民共和国反恐法》（以下简称《反恐法》）	第二十一条	电信、互联网、金融、住宿、长途客运、机动车租赁等业务经营者、服务提供者，应当对客户身份进行查验。对身份不明或拒绝身份查验的，不得提供服务
	第八十六条	电信、互联网、金融业务经营者、服务提供者未按规定对客户身份进行查验，或者对身份不明、拒绝身份查验的客户提供服务的，主管部门应当责令改正；拒不改正的，处二十万元以上五十万元以下罚款，并对其直接负责的主管人员和其他直接责任人员处十万元以下罚款；情节严重的，处五十万元以上罚款，并对其直接负责的主管人员和其他直接责任人员，处十万元以上五十万元以下罚款
《全国人大常委会关于加强网络信息保护的决定》	第六条	网络服务提供者为用户办理网站接入服务，办理固定电话、移动电话等入网手续，或者为用户提供信息发布服务，应当在与用户签订协议或确认提供服务时，要求用户提供真实身份信息
《中华人民共和国电信条例》（以下简称《电信条例》）	第五十八条	任何组织或个人不得有下列扰乱电信市场秩序的行为：（一）采取租用电信国际专线、私设转接设备或其他方法，擅自经营国际或香港特别行政区、澳门特别行政区和台湾地区电信业务；（二）盗接他人电信线路，复制他人电信号码，使用明知是盗接、复制的电信设施或号码；（三）伪造、变造电话卡及其他各种电信服务有价凭证；（四）以虚假、冒用的身份证件办理入网手续并使用移动电话
《电话用户真实身份登记规定》	第五条	电信业务经营者应当依法登记和保护电话用户办理入网手续时提供的真实身份信息

续表

法律名称	法律条款	法律规定
《电话用户真实身份登记规定》	第六条	电信业务经营者为用户办理入网手续时，应当要求用户出示有效证件、提供真实身份信息，用户应当予以配合。用户委托他人办理入网手续的，电信业务经营者应当要求受托人出示用户和受托人的有效证件，并提供用户和受托人的真实身份信息

二、网络实名制的法规遵从建议

根据我国《网络安全法》第二十四条规定，网络运营者为用户办理网络接入、域名注册服务，办理固定电话、移动电话等入网手续，或者为用户提供信息发布、即时通信等服务，在与用户签订协议或确认提供服务时，应当要求用户提供真实身份信息。用户不提供真实身份信息的，网络运营者不得为其提供相关服务。国家实施网络可信身份战略，支持研究开发安全、方便的电子身份认证技术，推动不同电子身份认证之间的互认。第六十一条还规定了相关的法律责任，具体遵从建议如表 6-2 所示。

表 6-2 网络实名制的法规遵从建议

控制项	网络实名制的法规遵从要求	对应条款
可信身份战略与实名制的要求	网络运营者为用户办理网络接入、域名注册服务，办理固定电话、移动电话等入网手续，或者为用户提供信息发布、即时通信等服务，在与用户签订协议或确认提供服务时，应当要求用户提供真实身份信息。用户不提供真实身份信息的，网络运营者不得为其提供相关服务。国家实施网络可信身份战略，支持研究开发安全、方便的电子身份认证技术，推动不同电子身份认证之间的互认	《网络安全法》第二十四条、第六十一条、第六十七条
责任承担	网络运营者违反本法第二十四条第一款规定，未要求用户提供真实身份信息，或者对不提供真实身份信息的用户提供相关服务的，由有关主管部门责令改正；拒不改正或情节严重的，处五万元以上五十万元以下罚款，并可以由有关主管部门责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款	
个人信息界定	本法下列用语的含义：（五）个人信息，是指以电子或其他方式记录的能够单独或与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等	

## 第四节 监督管理与法律责任

《网络安全法》第八条明确规定，国家网信部门负责统筹协调网络安全工作和相关监督管理工作。国务院电信主管部门、公安部门和其他有关机关依照本法和有关法律、行政法规的规定，在各自职责范围内负责网络安全保护和监督管理工作。县级以上地方人民政府有关部门的网络安全保护和监督管理职责，按照国家有关规定确定。

第六十一条规定，网络运营者违反本法第二十四条第一款规定，未要求用户提供真实身份信息，或者对不提供真实身份信息的用户提供相关服务的，由有关主管部门责令改正；拒不改正或情节严重的，处五万元以上五十万元以下罚款，并可以由有关主管部门责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。



# 网络安全监测预警和应急响应

全球化融合背景下，网络安全风险的范围、规模和复合程度大大增加，网络安全风险的动态性、不确定性和不可逆性要求对风险进行持续性监控，以有效实现风险控制的目标，而建立事前、事中、事后的网络安全风险防控体系对于新技术背景下的网络安全保障尤为必要。《国家网络空间安全战略》中明确要求完善网络安全监测预警和网络安全重大事件应急处置机制。

《网络安全法》重点关注网络安全监测预警和应急响应制度的建立和完善，一方面，在第二十五条、第五十一条、第五十二条、第五十四条、第五十五条中要求建立网络安全监测预警和信息通报制度，不仅确定了网络安全监测预警和信息通报的组织机构及其工作机制，重点强化了关键信息基础设施安全保护领域的网络安全监测预警和信息通报制度的构建，还明确了网络安全风险增大时省级政府有关部门应当采取的网络安全风险评估和预警措施，以及网络运营者的网络安全预警信息发布义务。另一方面，《网络安全法》还通过第五十三条、第五十五条、第五十六条、第五十七条、第五十八条建立了网络安全事件的应急响应制度，针对网络安全应急响应工作机制、网络安全应急预案的制定、网络安全事件的应急响应措施、约谈措施、网络安全事件引发的突发事件应对，以及网络通信临时管制措施都做出了明确的规定。由此可见，《网络安全法》已将网络安全监测预警和应急响应的规范性要求上升到了国家制度的高度，这是我国网络安全立法的重大突破。

## 第一节 网络安全监测与信息收集

### 一、《网络安全法》相关规定及释义

《网络安全法》第二十一条第三款要求网络运营者采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月。《网络安全法》第二十六条通过列举方式界定了网络安全信息的范围。《网络安全法》第五十一条明确要求国家建立网络安全监测预警和信息通报制度。实践中，要求国家安全、公安、工信、国家保密行政管理、国家密码管理等有关部门，网络运营者，关键信息基础设施的运营者，省级政府有关部门、机构和人员等采用技术手段实时监测其运营或主管的信息系统网络运行状态，及时收集和发现异常的网络安全事件及相关信息，如网络安全态势感知、脆弱性、入侵攻击事件及如何减少危害的信息等。

#### （一）网络安全监测的概念及其分类

网络安全监测，是指采用技术手段对网络与信息系统进行实时、动态且持续性的监控，以全面掌握网络的运行状态，发现网络入侵、攻击等网络安全风险的活动。网络安全监测是及时准确预警的前提和基础，通过监测研判的结果能够为预警提供科学的依据。全国网络安全标准化技术委员会《网络安全技术网络安全监测基本要求与实施指南（征求意见稿）》第4.2条规定，按照监测目标的不同，网络安全监测分为以下四类。①网络安全事件监测：对具有损害业务运作和威胁网络安全的事件，按照网络安全事件不同分类、分级要求，分析识别并进行展示与告警；②运行状态监测：对监测对象的运行状态进行实时捕捉，如各类设备和系统的可用性状态信息；③脆弱性与威胁监测：对监测对象的脆弱性、威胁进行评估分析，发现资产所面临的安全风险；④策略与配置监测：对各类设备和系统安全策略和配置信息进行核查分析，评估安全合规性情况。

## （二）网络安全监测信息的来源

《国家网络安全事件应急预案》明确要求，各有关部门按照“谁主管谁负责、谁运行谁负责”的要求，组织对本单位建设运行的网络和信息系统开展网络安全监测工作。重点行业主管或监管部门组织指导做好本行业网络安全监测工作。各省（区、市）网信部门结合本地区实际，统筹组织开展对本地区网络和信息系统的安全监测工作。各省（区、市）、各部门将重要监测信息报应急办，应急办组织开展跨省（区、市）、跨部门的网络安全信息共享。由此可见，网络安全监测预警和信息通报制度所涉及的网络安全信息来源于各有关部门的网络安全监测过程，即网络安全信息的来源主要包括自主监测信息和外部情报信息。参照工信部《互联网网络安全信息通报实施办法》和《公共互联网网络安全威胁监测与处置办法》，以及美国国家标准与技术研究院（National Institute of Standards and Technology, NIST）2014年发布的《网络威胁信息共享指南（草案）》[Guide to Cyber Threat Information Sharing (Draft)] 的相关规定，具体包括以下内容。

（1）自主监测信息，即由国家和地方政府有关部门、网络运营者、关键信息基础设施运营者等采用技术手段在对网络与信息系统进行实时、动态且持续性监控的过程中所获取的网络安全事件及潜在风险的相关信息。该类信息的来源包括入侵检测和防护系统、安全信息和事件管理产品、防病毒软件和文件完整性检查软件的警报，操作系统、网络、服务和应用的日志等，如异常的网络行为、DNS日志、防火墙溢出、Web代理日志、网络/Http日志。

（2）外部情报信息，来源于国家网信、公安、工信等政府有关部门，计算机应急响应小组，网络安全企业、科研机构及公众平台（如国家网络安全漏洞共享平台、乌云漏洞平台等）提供的网络安全情报信息，在特定领域内建立信息共享合作伙伴关系（如金融、电力、医疗等行业获得同样安全信息），以及从提供类似威胁情报和其他收费增值能力的商业网络威胁情报服务供应商处获得相关信息等。此外，还可通过互联网访问的公开安全信息公布危害指标信息、黑名单、恶意软件和病毒信息、垃圾邮件发送者名单，以及其他新出现的威胁等信息。

### （三）网络安全信息收集的内容

《网络安全法》第二十六条通过列举方式界定了网络安全信息，包括系统漏洞、计算机病毒、网络攻击、网络侵入等，这是从网络安全信息的技术类型角度给出的定义，体现了网络安全信息承载网络安全风险的基本功能。《网络安全法》第五十一条明确要求国家网信部门统筹协调有关部门加强网络安全信息收集工作，关键信息基础设施的运营者、省级政府有关部门等应当实时监测其运营或主管的信息系统网络运行状态，及时收集和发现异常的网络安全事件及相关信息，如网络态势感知、脆弱性、入侵事件及如何减少危害的信息等，尤其是涉及国家安全、公共健康和公共安全、国民经济及公众信心的已经发现或潜在的安全漏洞或网络威胁事件，并应当及时准确地掌握各种深层次、前瞻性的情报信息，以准确把握事件发生的规律和动态。具体而言，根据工信部《互联网网络安全信息通报实施办法》、《公共互联网网络安全威胁监测与处置办法》，以及美国 2015 年《网络安全信息共享法》等相关规定，网络安全信息收集的内容应当包括以下方面。

（1）安全事件信息：关于成功的或未遂的网络攻击的细节信息，包括丢失的信息、攻击中使用的技术、攻击意图、造成的影响等。安全事件所涵盖的范围从一次被成功封阻的攻击到造成严重国家安全危机的攻击。

（2）威胁信息：包括尚未认识清楚但可导致潜在严重影响的事项；门户网站、域名解析服务系统等网络基础设施发生阻断、瘫痪、拥堵、数据泄露、解析异常、域名劫持等异常情况；感染指标，如恶意文件、被窃取电子邮箱地址、受影响的 IP 地址、恶意代码样本；关于威胁实施者的信息。该类信息有助于发现安全事件，从攻击中吸取教训，创造解决方案等。

（3）漏洞信息：软件、硬件、商业流程中可被恶意利用的漏洞。

（4）态势感知信息：此类信息包括对被利用漏洞、活跃的威胁、攻击的实时遥测，还包括攻击目标、网络状况等信息，能够帮助决策人员响应安全事件。

## 二、网络安全监测与信息收集的制度概述

### （一）美国网络安全信息收集的立法实践

美国 2003 年《保护网络空间国家战略》(National Strategy to Secure Cyberspace)

要求联邦政府应当在政府和非政府中与网络空间安全有关的核心网络运行中心内安装网络预警和信息网,以供传播分析和预警信息,并负责完成危机协调工作。2006年《国家基础设施保护计划》(National Infrastructure Protection Plan, NIPP)提出了构建关键基础设施伙伴网络,共享国家基础设施相关预警信息,这一网络的核心是国家通信平台——国土安全信息网络(Homeland Security Information Network, HSIN),HSIN是由州和地方授权机构开发的涉及综合各种危害因素信息的共享通信系统,它连接了50个州、5个地域机构、华盛顿特区、50个主要城市区域。HSIN是通过通信、协调和信息共享等方式来加强国家关键基础设施保护,确保在其关键基础设施领域内或领域间,建立一个安全的、加密的且仅供官方使用的通信网络<sup>①</sup>。

具体而言,美国加强对网络安全事件的监测和信息收集主要有3种方式。①建立可信互联网连接,通过减少和整合联邦政府信息系统互联网外部出口连接数量,提高对互联网出口的监测和态势感知能力,加强对互联网出口的监测和管理。②部署爱因斯坦系统,为US-CERT和CERT团队提供实时的、更强的网络安全事件检测、收集、应急处置和报告的能力。③提高自动化管理水平,美国要求各联邦政府机构应具备监控安全相关信息的能力,这种能力应该是持续的、可管理及可控制的。为了实现这一目标,美国要求各政府机构加快安全相关行动的自动化进程并开发自动化的风险模型,以便在安全管理工具中将风险模型应用于系统弱点和威胁的识别。

## (二) 欧盟网络安全信息收集的立法实践

2005年《保护关键基础设施的欧洲计划》(The European Programme for Critical Infrastructure Protection, EPCIP)提出建立关键基础设施预警信息网络,以安全的方法为最好的实践交流提供一个平台。2009年《关键信息基础设施保护——保护欧洲免受大规模网络攻击和中断:预备、安全和恢复力的通信》(Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection “Protecting Europe from Large Scale Cyber-Attacks and Disruptions: Enhancing Preparedness, Security And Resilience”)

<sup>①</sup> 王玥,方婷,马民虎.美国关键基础设施信息安全监测预警机制演进与启示[J].情报杂志,2016,35(4):17-23.

中进一步提出五个支柱以应对关键基础设施面临的挑战，其中要求建立适当的早期预警机制和欧洲信息共享和预警系统，以落实检测和响应的具体要求。

此外，监测预警是欧盟应对网络攻击最主要的治理机制。针对网络攻击的监测是指在欧盟层面和各成员国层面通过单项指标预警与综合指标预警等两种方法，以及其他技术手段对网络攻击与信息系统攻击中的异常现象进行监测报告，并在此基础上建立针对网络系统和信息系统攻击的走向趋势的预判。在欧洲议会和欧盟理事会《关于信息系统攻击并取代理事会第 2005/222/JHA 号框架决定的第 2013 /40 /EU 号指令》(Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on Attacks against Information Systems and Replacing Council Framework Decision 2005/222/JHA) 中，对信息系统攻击的监测预警主要体现在两个方面：监控与统计 (Monitoring and Statistics)、信息系统漏洞的检测与报告 (Information System Vulnerability Detection and Reporting)。其中关于信息系统网络攻击的监测机制主要是与犯罪有关的数据的监控及统计，具体是指在涉及非法访问信息系统、非法系统干扰、非法数据干扰、非法拦截和用于犯罪的工具等犯罪时，各成员应记录 (Recording)、生成 (Production) 并提供 (Provision) 与此类型有关的犯罪统计数据及以该罪行起诉并定罪的人数。值得注意的是，欧洲议会和欧盟理事会指出，统计的数据应该遵从最小化原则，即监控与统计的数据应该符合比例原则，不得收集涉及公民的个人隐私等与犯罪无关的不必要信息。

### 三、网络安全监测与信息收集的法规遵从框架及建议

根据《网络安全法》及相关法律法规的要求，一方面，建设和运行网络安全威胁监测处置平台，实现对国际出入口、境内骨干网络核心节点的网络安全威胁监测，能够有效提高对各类网络攻击威胁和安全事件的及时发现、有效处置和准确溯源能力。另一方面，通过多种方式收集多种类型的数据，以及遵从网络安全监测日志的最低存留期限要求都是企业应当重点关注和履行的法规遵从义务。

网络安全监测与信息收集的法规遵从框架如表 7-1 所示。

表 7-1 网络安全监测与信息收集的法规遵从框架

法律名称	法律条款	法律规定
《网络安全法》	第二十一条	采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月
	第二十六条	开展网络安全认证、检测、风险评估等活动，向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息，应当遵守国家有关规定
	第五十一条	国家建立网络安全监测预警和信息通报制度。国家网信部门应当统筹协调有关部门加强网络安全信息收集、分析和通报工作，按照规定统一发布网络安全监测预警信息
	第五十二条	负责关键信息基础设施安全保护工作的部门，应当建立健全本行业、本领域的网络安全监测预警和信息通报制度，并按照规定报送网络安全监测预警信息
《关键信息基础设施安全保护条例（征求意见稿）》	第二十三条	采取技术措施，监测、记录网络运行状态、网络安全事件，并按照规定留存相关的网络日志不少于六个月
	第三十六条	国家网信部门统筹建立关键信息基础设施网络安全监测预警体系和信息通报制度，组织指导有关机构开展网络安全信息汇总、分析研判和通报工作，按照规定统一发布网络安全监测预警信息
	第三十七条	国家行业主管或监管部门应当建立健全本行业、本领域的关键信息基础设施网络安全监测预警和信息通报制度，及时掌握本行业、本领域关键信息基础设施运行状况和安全风险，向有关运营者通报安全风险和相关工作信息
《密码法（草案征求意见稿）》	第十九条	密码管理部门和有关部门建立密码安全监测预警、信息通报、重大事项会商和应急处置机制，确保密码安全管理的协同联动和有序高效
《国家网络安全事件应急预案》	3.2 预警监测	各单位按照“谁主管谁负责、谁运行谁负责”的要求，组织对本单位建设运行的网络和信息系统开展网络安全监测工作。重点行业主管或监管部门组织指导做好本行业网络安全监测工作。各省（区、市）网信部门结合本地区实际，统筹组织开展对本地区网络和信息系统的安全监测工作。各省（区、市）、各部门将重要监测信息报应急办，应急办组织开展跨省（区、市）、跨部门的网络安全信息共享
《互联网网络安全信息通报实施办法》	第七条	基础电信业务经营者、跨省经营的增值电信业务经营者、CNCERT、互联网域名注册管理机构、互联网域名注册服务机构应建立并完善本单位信息监测机制，提高监测能力，自主监测涉及本单位管理范围内的信息
	第二十三条	CNCERT 应与网络安全研究机构、网络安全技术支撑单位、非经营性互联单位、网络安全企业、国际网络安全组织等广泛合作，积极拓展网络安全信息获取渠道

续表

法律名称	法律条款	法律规定
《工业控制系统信息安全事件应急管理工作指南》	第十一条	工业和信息化部指导国家工业信息安全发展研究中心等技术机构，组织开展全国工控安全风险监测、预警通报等工作，提升情报收集、态势分析、风险评估和信息共享能力。 地方工业和信息化主管部门组织开展本地区工控安全风险监测工作。工业企业组织开展本单位工控安全风险监测工作
《工业控制系统信息安全防护指南》	第七条	在工业控制网络部署网络安全监测设备，及时发现、报告并处理网络攻击或异常行为
《通信网络安全防护管理办法》	第十五条	通信网络运行单位应当建设和运行通信网络安全监测系统，对本单位通信网络的安全状况进行监测
《公共互联网网络安全威胁监测与处置办法》	第二条	本办法所称公共互联网网络安全威胁是指公共互联网上存在或传播的、可能或已经对公众造成危害的网络资源、恶意程序、安全隐患或安全事件，包括： （一）被用于实施网络攻击的恶意 IP 地址、恶意域名、恶意 URL、恶意电子信息，包括木马和僵尸网络控制端，钓鱼网站，钓鱼电子邮件、短信/彩信、即时通信等； （二）被用于实施网络攻击的恶意程序，包括木马、病毒、僵尸程序、移动恶意程序等； （三）网络服务和产品中存在的安全隐患，包括硬件漏洞、代码漏洞、业务逻辑漏洞、弱口令、后门等； （四）网络服务和产品已被非法入侵、非法控制的网络安全事件，包括主机受控、数据泄露、网页篡改等； （五）其他威胁网络安全或存在安全隐患的情形
	第三条	工业和信息化部负责组织开展全国公共互联网网络安全威胁监测与处置工作。各省、自治区、直辖市通信管理局负责组织开展本行政区域内公共互联网网络安全威胁监测与处置工作。工业和信息化部 and 各省、自治区、直辖市通信管理局以下统称为电信主管部门
	第四条	网络安全威胁监测与处置工作坚持及时发现、科学认定、有效处置的原则
	第五条	相关专业机构、基础电信企业、网络安全企业、互联网企业、域名注册管理和服务机构等应当加强网络安全威胁监测与处置工作，明确责任部门、责任人和联系人，加强相关技术手段建设，不断提高网络安全威胁监测与处置的及时性、准确性和有效性
	第六条	工业和信息化部建立网络安全威胁信息共享平台，统一汇集、存储、分析、通报、发布网络安全威胁信息；制定相关接口规范，与相关单位网络安全监测平台实现对接。国家计算机网络应急技术处理协调中心负责平台建设和运行维护工作



针对网络安全监测与信息收集的法规遵从建议，表 7-2 梳理了网络安全监测信息采集、存储及实施过程当中的技术、环境和性能等具体要求，以及网络运营者在履行网络安全监测与信息收集义务时应当重点关注的方面。

表 7-2 网络安全监测与信息收集的法规遵从建议

控制项	网络安全监测与信息收集的法规遵从建议	对应条款
1. 网络安全监测信息采集		<p>第二十一条 国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或未经授权的访问，防止网络数据泄露或被窃取、篡改：</p> <p>（三）采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月。</p> <p>第五十一条 国家建立网络安全监测预警和信息通报制度。国家网信部门应当统筹协调有关部门加强网络安全信息收集、分析和通报工作，按照规定统一发布网络安全监测预警信息。</p> <p>第五十二条 负责关键信息基础设施安全保护工作的部门，应当建立健全本行业、本领域的网络安全监测预警和信息通报制度，并按照规定报送网络安全监测预警信息</p>
采集的技术要求	组织应通过日志采集、协议采集、包采集等方式采集日志数据、性能数据、流数据、威胁数据、配置数据、脆弱性数据、包数据、策略数据等多种类型数据，并将采集到的数据转化为标准化数据格式	
采集的环境要求	组织应建立采集引擎，支持多种协议解析，以主动和被动的采集结构化数据、非结构化数据和半结构化数据；支持实时采集与批量采集等多种采集模式；主动方式应以最小权限获取数据	
采集的性能要求	组织应确保采集组件的部署依据邻近采集原则，避免跨多个网络区域数据采集，应依据一次性采集原则，不对同一对象客体数据重复采集。 组织应确保安全监测采集功能在满足安全监测采集范围、种类、频次等需求基础上，采集功能规划设计依据最小影响原则，不对应采集客体的运行造成不必要影响。例如，组织应确保对被采集对象的内存资源占用率不超过 5%。 组织应保证至少有一个采集节点正常工作	
2. 网络安全监测信息存储		
存储的技术要求	组织应按照如下要求设计网络安全监测信息的存储模块： 具备数据预处理功能，包括格式化处理、补充上下文信息（如用户、地理位置和区域）、数据发布等； 具备分布式存储功能，要能够将不同类型的异构数据进行分类存储，如归一化日志、流量元数据、PCAP 文件； 支持按需扩展存储节点； 满足可靠性、并发性的要求，并进行备份存储； 监测数据中的重要信息应进行处理保证数据保密性； 监测数据应采取校验机制保证数据完整性； 采取备份机制保证重要监测数据的可用性； 对监测数据设置访问权限，按权限限定监测数据使用； 根据具体情况对监测数据设定保存期限，并按照规定（不少于六个月）对数据进行存储； 对存储数据结构进行规划设计，对外部系统、上下级系统提供存储对接接口	

续表

控制项	网络安全监测与信息收集的法规遵从建议	对应条款
存 储 的 环 境 要求	组织应通过数据库方式存储数据，支持原格式数据存储。存储信息应包含原始数据库、资产数据库、安全事件库、预警与告警数据库、规则数据库等	
存 储 的 性 能 要求	组织应根据采集对象种类、数量、采集要求估算系统数据的采集存储需求，需要分别针对采集原始数据、监测过程数据、监测结果数据规划存储容量要求；并根据数据用途规划在线数据存储容量和离线存储容量。  组织应保证至少一个存储管理节点正常运行且另一个节点 30 分钟内恢复正常使用。组织应确保数据的保存期限不少于六个月；数据存储具体备份和灾难恢复能力；重要数据应加密存储	
3. 网络安全监测实施		
网络安全监测实施主体	组织应确定其网络安全监测实施主体，并根据主体范围设计监测方案。例如，针对其网络管理人员、系统管理人员、数据库管理人员、应用管理人员、业务管理人员等设计不同的监测方案	
技术实施合规分析	组织应确保监测技术的实施符合国家及监管部门的安全管理规范，遵守保护企业单位、个人隐私信息的保护要求	
外部机构支持协作	组织应确定其网络安全监测与信息收集的外部支持资源，如与外部机构同步重大网络攻击事件信息、典型安全漏洞信息、恶意网站地址信息等；  组织应确定其基础数据来源，如网络解析域名信息、网络实名信息等，并根据网络安全监测需求，与外部支持机构确定获取支持数据的方式方法	

四、监督管理与法律责任

《网络安全法》第八条第一款规定，国家网信部门负责统筹协调网络安全工作和相关监督管理工作。具体而言，为了协调国家有关部门网络安全监测和信息收集工作的协同性和一致性，《网络安全法》第五十一条规定，国家网信部门应当统筹协调有关部门加强网络安全监测和信息收集工作，这是由网络安全管理工作的特点决定的。网络安全管理工作涉及诸多相关部门，包括国家安全、公安、工信、国家保密行政管理、国家密码管理等，而网络安全信息来源分散、数据体量大，要求上述各有关部门除了在其职责范围内负责落实网络安全监测与信息收集工作之外，还要加强各部门相互之间的沟通协作，接受国家网信部门在网络安全监测

与信息收集工作方面的统筹协调。此外，工信部《公共互联网网络安全威胁监测与处置办法》规定，工业和信息化部负责组织开展全国公共互联网网络安全威胁监测与处置工作。各省、自治区、直辖市通信管理局负责组织开展本行政区域内公共互联网网络安全威胁监测与处置工作。

在法律责任方面，针对违反网络安全监测与信息收集的相关规定，没有按照《网络安全法》第二十一条第三款规定的最低期限进行监测日志留存的，由网络运营者的有关主管部门责令改正，给予警告；拒不改正或导致危害网络安全等后果的，处一万元以上十万元以下罚款，对直接负责的主管人员处五千元以上五万元以下罚款。

## 第二节 网络安全信息分析与预警研判

### 一、《网络安全法》相关规定及释义

《网络安全法》第五十四条第二款规定，网络安全事件发生的风险增大时，省级以上人民政府有关部门应当按照规定的权限和程序，并根据网络安全风险的特点和可能造成的危害，组织有关部门、机构和专业人员，对网络安全风险信息进行分析评估，预测事件发生的可能性、影响范围和危害程度。根据工信部《互联网网络安全信息通报实施办法》第十条规定，网络安全信息通报的内容应当包括事件信息和预警信息。其中预警信息是指存在潜在安全威胁或隐患但尚未造成实际危害和影响的信息，或者对事件信息分析后得出的预防性信息。基于此，部分预警信息的获取实际上基于对所收集获取的事件信息所进行的分析研判。此外，《国家网络安全事件应急预案》规定，各省（区、市）、各部门组织对监测信息进行研判，认为需要立即采取防范措施的，应当及时通知有关部门和单位，对可能发生重大及以上网络安全事件的信息及时向应急办报告。各省（区、市）、各部门可根据监测研判情况，发布本地区、本行业的橙色及以下预警。应急办组织研判，确定和发布红色预警和涉及多省（区、市）、多部门、多行业的预警。

目前，我国已经建立了以国家网络与网络安全信息通报中心为核心，包括公安部网络安全等级保护评估中心、国家互联网应急中心、中国网络安全认证中心、中国网络安全测评中心、公安部计算机信息系统安全产品质量监督检验中心、计算机病毒防治产品检验中心等在内的机构，负责对网络安全事件进行监测、通报、预警、处置和宣传。然而，网络安全工作涉及部门众多，网络安全信息来源分散、数据量大，且有关网络安全信息的分析报告数据分散在各个部门，例如公安部、工信部等分别掌握着自己的数据，没有一个系统的、全面的、深入的数据分析机构，导致各自分析各自的数据，出具各自的报告，造成态势分析的片面性和不及时性。

## 二、网络安全信息分析与预警研判的制度概述

各国高度关注对其收集和获取的网络安全信息进行整合分析的能力，以为有效应对网络安全威胁提供重要支撑。有些国家设立了永久性分析和情报中心，旨在更有效地向公共和私有部门的决策者提供战略信息，如美国的信息共享与分析中心和日本的通信信息共享与分析中心。

美国 2003 年《保护网络空间国家战略》（National Strategy to Secure Cyberspace）重点要求从战术和战略上为分析网络攻击及脆弱性评估做准备，其中指出分析是深入了解网络安全事件及攻击的第一步，包括攻击的本质、泄露的信息和造成破坏的规模，以及与攻击者的意图、使用的工具、利用的脆弱性相关的线索。具体而言，针对网络空间的分析包括战术分析、战略分析和脆弱性评估三类。战术分析将通过分析网络安全事件相关的事实，找出脆弱性并提出预警，如分析计算机病毒的传播原理以及时找到保护或减轻破坏的方法。战略分析不是分析特定的事件，而是更广泛地研究大量的事件及其背后的含义，判断事件对整个国家可能造成的影响。例如，针对网络安全威胁和脆弱性的长期发展趋势进行分析，并据此就新的攻击方法等正在增加的攻击发出预警，此外，战略分析同时还为政策制定人员提供了信息，使其能够对未来的攻击进行预测并做好准备，由此可以减少攻击造成的破坏。脆弱性评估是指对网络空间及其物理设施进行详细的检查以发现并研究其弱点，使得基础设施拥有者和运营者能够增强其对各种威

胁的抵抗能力。

2006年《国家基础设施保护计划》(National Infrastructure Protection Plan, NIPP)要求根据相关法律规定和信息保护责任以安全的方式分析、存储和共享风险评估数据。同时,优先性关注收集和分析风险评估结果,以明确资产、系统和网络风险的全面情况,建立基于风险的优先次序,并提供最有效的风险缓解措施,以确定保护和业务连续性计划。

2015年2月,美国总统奥巴马要求国家情报总监成立网络威胁与情报整合中心(Cyber Threat Intelligence Integration Center, CTIIC),该机构协调整合了国土安全部、联邦调查局、中央情报局、国家安全局等多部门的情报力量,旨在对影响美国国家利益的国外网络威胁和网络事件提供整合的全源情报分析。

### 三、网络安全信息分析与预警研判的法规遵从框架及建议

为了避免“信息孤岛”、“信息壁垒”等现象的出现,现行的网络安全管理法律法规要求相关部门在履行各自职责的基础上对本部门内部收集的及来源于外部的网络安全威胁、漏洞和事件信息等网络安全信息进行整合分析。例如,工信部《互联网网络安全信息通报实施办法》规定,CNCERT在接到预警信息后,应立即组织对预警信息进行跟踪、分析,有重要情况应及时向通信保障局报告。第十七条规定,通信保障局根据信息性质、内容、紧急程度等,必要时组织相关单位、专家对信息进行研判。

实践中,政府各有关部门、CNCERT等机构组织、网络安全企业、网络安全研究机构等企业之间应当建立网络安全信息分析的合作伙伴关系,利用各参与主体的技术能力和资源优势对其掌握的网络安全信息进行分析研判,能够为预警信息发布提供有力支撑。网络安全信息分析要求国家政府有关部门组织网络安全主管部门、机构的专业人员,网络运营者,关键信息基础设施的运营者、网络安全服务机构等对所获得的网络安全风险信息进行系统的分析评估,针对网络安全事件发生的可能性进行预测,并对网络安全事件发生后的影响程度,包括影响主体、影响持续时间、影响业务范围、地域范围、级别等进行预测,制定网络安全事件

预测评估分析报告<sup>①</sup>。

网络安全信息分析的法规遵从框架如表 7-3 所示。

表 7-3 网络安全信息分析的法规遵从框架

法律名称	法律条款	法律规定
《网络安全法》	第五十一条	国家建立网络安全监测预警和信息通报制度。国家网信部门应当统筹协调有关部门加强网络安全信息收集、分析和通报工作，按照规定统一发布网络安全监测预警信息
	第五十二条	负责关键信息基础设施安全保护工作的部门，应当建立健全本行业、本领域的网络安全监测预警和信息通报制度，并按照规定报送网络安全监测预警信息
	第五十四条	网络安全事件发生的风险增大时，省级以上人民政府有关部门应当按照规定的权限和程序，并根据网络安全风险的特点和可能造成的危害，采取下列措施： (二) 组织有关部门、机构和专业人员，对网络安全风险信息进行分析评估，预测事件发生的可能性、影响范围 and 危害程度
《关键信息基础设施安全保护条例（征求意见稿）》	第三十六条	国家网信部门统筹建立关键信息基础设施网络安全监测预警体系和信息通报制度，组织指导有关机构开展网络安全信息汇总、分析研判和通报工作，按照规定统一发布网络安全监测预警信息
《互联网网络安全信息通报实施办法》	第十条	报送的信息分为事件信息和预警信息。 事件信息是指已经发生的网络安全事件信息。 预警信息是指存在潜在安全威胁或隐患但尚未造成实际危害和影响的的信息，或者对事件信息分析后得出的预防性信息
《工业控制系统信息安全事件应急管理工作指南》	第十一条	工业和信息化部指导国家工业信息安全发展研究中心等技术机构，组织开展全国工控安全风险监测、预警通报等工作，提升情报搜集、态势分析、风险评估和信息共享能力
	第十二条	地方工业和信息化主管部门、工业企业定期将重要监测信息报国家工业信息安全发展研究中心，国家工业信息安全发展研究中心负责汇总、整理和研判，并将结果报工业和信息化部；针对可能超出本地区应对能力范围的安全风险和事件信息，及时上报，必要时工业和信息化部协调应急技术机构提供支持
《国家网络安全事件应急预案》	3.3 预警研判和发布	各省（区、市）、各部门组织对监测信息进行研判，认为需要立即采取防范措施的，应当及时通知有关部门和单位，对可能发生重大及以上网络安全事件的信息及时向应急办报告。各省（区、市）、各部门可根据监测研判情况，发布本地区、本行业的橙色及以下预警

① 杨合庆. 中华人民共和国网络安全法释义[M]. 北京：中国民主法制出版社，2017.

根据监测目标的不同，网络安全监测分为信息安全事件监测、运行状态监测、脆弱性与威胁监测、策略与配置监测。基于此，全国信息安全标准化技术委员会《信息安全技术 网络安全监测基本要求与实施指南（征求意见稿）》的第 5.3 条规定，采集到的数据应从安全事件、运行状态、脆弱性与威胁、策略与配置方面进行分析，发现安全事件或威胁。表 7-4 描述了网络安全信息分析的法规遵从建议。

表 7-4 网络安全信息分析的法规遵从建议

控制项	网络安全信息分析的法规遵从建议	对应条款
1. 网络安全信息分析的技术要求		
安全事件分析	<p>组织应采用多种关联分析技术综合分析，发现病毒感染、恶意代码、数据泄露、攻击入侵、设备故障、系统状态变化、人员违规行为与误操作等安全事件或风险；</p> <p>组织应具备安全事件关联分析能力，通过关联分析比对识别异常行为；</p> <p>组织应基于流量基线检测异常的能力，识别网络访问、违规访问、访问频次和访问路径等异常；</p> <p>组织应具备 Web 异常检测功能，通过 HTTP 协议流量分析、检测渗透行为；</p> <p>组织应具备邮件异常检测能力，通过对 SMTP/POP3/IMAP 协议流量分析、检测基于电子邮件的外部渗透行为；</p> <p>组织应按照其内部对事件分类分级的方法，对安全事件进行相应的分类分级，并按照流程进行处置分析</p>	<p>第五十四条 网络安全事件发生的风险增大时，省级以上人民政府有关部门应当按照规定的权限和程序，并根据网络安全风险的特点和可能造成的危害，采取下列措施：</p> <p>（二）组织有关部门、机构和专业人员，对网络安全风险信息进行分析评估，预测事件发生的可能性、影响范围和危害程度</p>
运行状态分析	<p>组织应进行满足实际需求的运行状态监控，通过可视化图表查看监控信息；设置告警阈值；并进行运行状态的历史分析；</p> <p>组织应进行各种运行状态指标的对比分析，提供基于时间段、基于资产等不同维度的对比分析，并进行动态直观展示；</p> <p>组织应通过安全管控、安全审计、健康性评估等对系统运行状态管理分析</p>	
脆弱性与威胁分析	<p>组织应具备脆弱性感知能力，对资产进行脆弱性检测和数据展示；根据不同维度进行展示，包括单个资产、安全域、信息系统等维度；</p> <p>组织应具备威胁感知能力，对威胁进行展示和关联，包括已（未）遭受到的威胁；已遭受威胁需要对威胁进行分类，提取出关键威胁指标，提供组织的威胁态势；未遭受威胁需要对外部威胁情报进行分类展示、关联，提供与组织相关的位置威胁分析；</p> <p>组织应具备威胁判定能力，将多个威胁进行关联分析和评估</p>	
策略与配置分析	<p>组织应通过策略与配置的对比分析，分析配置的符合性；</p> <p>组织应通过配置的变更分析，获取配置的动态变化进行审核监测</p>	

续表

控制项	网络安全信息分析的法规遵从建议	对应条款
2. 网络安全信息分析的环境要求		
	组织应建立数据格式化引擎和分析引擎，通过数据格式化引擎对数据进行清洗、去噪、去重、归并、数据格式化等操作，分析引擎应具备聚类、分类、关联分析、深度学习等能力，可对数据进行统计、分析、挖掘和深度学习	
3. 网络安全信息分析的性能要求		
	组织应确保数据处理及分析功能设计满足用户对数据处理、分析的可扩展、可定义需求	

四、监督管理与法律责任

《网络安全法》第八条规定，国家网信部门负责统筹协调网络安全工作和相关监督管理工作。国务院电信主管部门、公安部门和其他有关机关依照本法和有关法律、行政法规的规定，在各自职责范围内负责网络安全保护和监督管理工作。县级以上地方人民政府有关部门的网络安全保护和监督管理职责，按照国家有关规定确定。《网络安全法》第五十一条规定，国家网信部门应当统筹协调有关部门加强网络安全信息分析工作。上述规定表明国家安全、公安、工信、国家保密行政管理、国家密码管理等有关部门除了在其职责范围内负责落实网络安全信息分析和预警研判工作之外，相互之间还要加强在此方面的沟通与协作，接受国家网信部门在网络安全信息分析和预警研判工作方面的统筹协调，以增强国家整体的安全态势感知能力。

第三节 网络安全信息通报

一、《网络安全法》相关规定及释义

网络安全事件本身固有的突发性、破坏性强的特点决定了必须建立快速有效的网络安全信息通报制度。网络安全信息通报制度对网络安全监测预警具有重要



意义，发挥着跨部门、多层级的信息交流与共享平台的作用，是协调有关部门，整合多方资源，实现综合防控、主动防范的重要载体。网络安全信息通报是网络安全管理过程当中传递信息、积极防范、协调联通、综合防御的有效手段，也是国家网络安全管理的基础性工作。《网络安全法》第二十五条、第五十一条、第五十二条和第五十四条分别要求建立国家层面、关键行业和领域，省级以上政府有关部门，以及网络运营者之间的全国立体的网络安全监测预警相对应的网络安全信息通报制度。

《网络安全法》第二十五条规定，在发生危害网络安全的事件时，网络运营者立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告。第五十二条规定，负责关键信息基础设施安全保护工作的部门，应当建立健全本行业、本领域的网络安全监测预警和信息通报制度，并按照规定报送网络安全监测预警信息。由此可见，《网络安全法》要求构建全国立体的网络安全监测预警的信息通报制度，包括国家网信部门、负责关键信息基础设施安全保护的工作部门、省级人民政府及其有关部门，以及网络运营者之间自上而下的信息通知（通告）和自下而上的信息报送（报告），以促使上述主体之间实现互联互通，加强跨部门、跨地区的信息交流与情报合作，提高国家整体对网络安全威胁的发现能力、预警能力、防护能力和反制能力。

## 二、网络安全信息通报的法规遵从框架及建议

根据相关法律法规的要求，网络安全信息通报的法规遵从框架重点围绕以下几个方面：第一，网络安全信息通报应遵循及时、客观、真实、准确、完整的原则，不得迟报、谎报、瞒报、漏报；第二，网络运营者应当制定和完善其内部的信息通报机制，包括明确负责网络安全信息通报工作的主管领导和承担信息通报工作的责任部门、负责人和联络人等；第三，针对需要报送的信息应当进行分类、分级，并根据分类分级的相应规定报送相关信息；第四，网络安全信息通报原则上应以书面方式或可验证来源的电子方式等形式为准，紧急情况可以先电话联系，后补书面报告；第五，网络安全信息通报的内容包括事件信息和预警信息，其中事件信息是指已经发生的网络安全事件信息，预警信息是指存在潜在安全威胁或隐患

但尚未造成实际危害和影响的信息，或者对事件信息分析后得出的预防性信息。

网络安全信息通报的法规遵从框架如表 7-5 所示。

表 7-5 网络安全信息通报的法规遵从框架

法律名称	法律条款	法律规定
《网络安全法》	第二十五条	网络运营者应当制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险；在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告
	第五十一条	国家建立网络安全监测预警和信息通报制度。国家网信部门应当统筹协调有关部门加强网络安全信息收集、分析和通报工作，按照规定统一发布网络安全监测预警信息
	第五十二条	负责关键信息基础设施安全保护工作的部门，应当建立健全本行业、本领域的网络安全监测预警和信息通报制度，并按照规定报送网络安全监测预警信息
	第五十四条	网络安全事件发生的风险增大时，省级以上人民政府有关部门应当按照规定的权限和程序，并根据网络安全风险的特点和可能造成的危害，采取下列措施： (一) 要求有关部门、机构和人员及时收集、报告有关信息，加强对网络安全风险的监测
《关键信息基础设施安全保护条例（征求意见稿）》	第三十六条	国家网信部门统筹建立关键信息基础设施网络安全监测预警体系和信息通报制度，组织指导有关机构开展网络安全信息汇总、分析研判和通报工作，按照规定统一发布网络安全监测预警信息
	第三十七条	国家行业主管或监管部门应当建立健全本行业、本领域的关键信息基础设施网络安全监测预警和信息通报制度，及时掌握本行业、本领域关键信息基础设施运行状况和安全风险，向有关运营者通报安全风险和相关工作信息
《密码法（草案征求意见稿）》	第十九条	密码管理部门和有关部门建立密码安全监测预警、信息通报、重大事项会商和应急处置机制，确保密码安全管理的协同联动和有序高效
《国家网络安全事件应急预案》	4.1 事件报告	网络安全事件发生后，事发单位应立即启动应急预案，实施处置并及时报送信息。各有关地区、部门立即组织先期处置，控制事态，消除隐患，同时组织研判，注意保存证据，做好信息通报工作。对于初判为特别重大、重大网络安全事件的，立即报告应急办
《互联网网络安全信息通报实施办法》	第六条	信息报送应遵循及时、客观、真实、准确、完整的原则，不得迟报、谎报、瞒报、漏报
	第八条	信息报送单位应制定并完善本单位信息通报机制，明确负责信息通报工作的主管领导和承担信息通报工作的责任部门、负责人和联络人，及时汇总本单位内部不同部门、不同渠道掌握的网络安全信息。信息报送单位应将本单位信息通报机制报通信保障局备案

续表

法律名称	法律条款	法律规定
《互联网网络安全信息通报实施办法》	第十条	报送的信息分为事件信息和预警信息。 事件信息是指已经发生的网络安全事件信息。 预警信息是指存在潜在安全威胁或隐患但尚未造成实际危害和影响的信息，或者对事件信息分析后得出的预防性信息
	第十一条	事件信息分为特别重大、重大、较大、一般共四级。预警信息分为一级、二级、三级、四级，分别用红色、橙色、黄色、蓝色标识，一级为最高级。具体分级规范见附件二，通信保障局负责对分级规范进行修订
	第十二条	信息报送单位应按照本办法第十条、第十一条规定对信息进行分类、分级，并根据本办法的相应规定报送信息。 基础电信业务经营者集团公司负责汇总、核实、报送省级分公司/子公司的信息。省级分公司/子公司将信息同时抄送当地通信管理局
	第十三条	对于特别重大、重大事件信息以及一级、二级预警信息，信息报送单位应于 2 小时内向通信保障局及相关通信管理局报告，抄送 CNCERT。 对于较大事件信息以及三级预警信息，信息报送单位应当于 4 小时内向相关通信管理局报告，抄送 CNCERT；对于跨省（自治区、直辖市）的较大事件信息，应同时向通信保障局报告。 对于一般事件信息，信息报送单位应按月及时汇总，于次月 5 个工作日内报送 CNCERT，抄送相关通信管理局；对于四级预警信息，信息报送单位应当于发现或得知预警信息后 5 个工作日内报送 CNCERT，抄送相关通信管理局
	第十四条	事件信息报送的内容应包括： （一）事件发生单位概况； （二）事件发生时间； （三）事件简要经过； （四）初步估计的危害和影响； （五）已采取的措施； （六）其他应当报告的情况
	第十五条	预警信息报送的内容应包括： （一）信息基本情况描述； （二）可能产生的危害及程度； （三）可能影响的用户及范围； （四）截至信息报送时，已知晓该信息的单位/人员范围； （五）建议应采取的应对措施及建议
	第十六条	事件发生后出现新情况的，信息报送单位应当及时补报。 CNCERT 在接到预警信息后，应立即组织对预警信息进行跟踪、分析，有重要情况应及时向通信保障局报告

续表

法律名称	法律条款	法律规定
《互联网网络安全 信息通报实施办法》	第十八条	各单位应以书面形式报送信息，并加盖单位公章。紧急情况可以先电话联系，后补书面报告
	第十九条	对于特别重大、重大、较大事件信息及一级、二级、三级预警信息，由通信保障局审核后，根据有关规定直接或委托 CNCERT 及时通告相关单位、人员或互联网用户，并抄送各通信管理局。 对于一般事件信息，由 CNCERT 负责汇总、分析全部信息，于次月 10 个工作日内将当月信息向通信保障局报送，向相关单位、人员通告，并抄送各通信管理局；对于四级预警信息，由 CNCERT 根据实际情况及时向相关单位、人员通告，并抄送各通信管理局
	第二十条	事件信息通告内容主要包括事件统计情况、造成的危害、影响程度、态势分析、典型案例。 预警信息通告内容主要包括受影响的系统、可能产生的危害和危害程度、可能影响的用户及范围、建议应采取的应对措施及建议
	第二十一条	信息报送单位应将本单位信息通报工作主管领导，责任部门负责人、联系人、联系方式报送通信保障局，抄送 CNCERT。以上信息发生变更，应在 3 个工作日内报送变更情况
	第二十二条	通信保障局建立会商制度，通报当前网络安全情况，与相关单位和专家研讨网络安全形势、网络安全问题及其应对策略等
	附件一：信息报送项目 (一) 基础电信业务经营者	(1) 本单位提供互联网接入服务的普通电信用户、专线用户、重要信息系统用户业务发生阻断、拥塞等异常情况。 (2) 本单位 IP 基础网络设施，包括互联网国际设施、国内互联网设备和链路、IDC 等发生瘫痪、阻断等异常情况。 (3) 本单位域名解析服务系统发生瘫痪、解析异常、域名劫持等异常情况。 (4) 本单位网上营业厅、门户网站、移动 WAP 类业务，或者与互联网相连的网络和系统发生系统瘫痪、阻断、用户数据丢失等异常情况。 (5) 影响互联网业务正常运营、影响用户正常访问互联网、造成重大社会影响和经济损失等异常情况。 (6) 本单位网内漏洞等网络安全隐患及处置情况。 (7) 本单位网内发生拒绝服务攻击或其他流量异常事件情况。 (8) 本单位网内木马和僵尸网络、病毒等恶意代码传播情况。 (9) 本单位网内路由系统出现的路由劫持情况（路由劫持是指若同一 IP 地址前缀有多个自治系统为宣告者，且自治系统之间无隶属关系或未得到该 IP 地址前缀的授权，则判定为域间路由劫持）。 (10) 本单位垃圾邮件监测、预警和处置情况。 (11) 获知的由本单位提供服务的重要信息系统用户内部发生的网络安全异常情况。 (12) 通过各种渠道获得的其他信息

续表

法律名称	法律条款	法律规定
《互联网网络安全信息通报实施办法》	附件一：信息报送项目  (二) 互联网域名注册管理、服务机构	(1) 本单位域名系统解析服务异常等情况，包括系统稳定性、解析成功率、响应时间、解析数据和数据库等方面出现的异常情况。 (2) 网页挂马、网络仿冒、域名劫持等网络安全事件。 (3) 域名系统相关的系统漏洞等网络安全风险信息及处置情况。 (4) 可疑域名或域名注册行为等情况。 (5) 通过各种渠道获得的其他信息
	附件一：信息报送项目  (三) 增值电信业务经营者 (IDC、门户网站、搜索引擎服务提供商等)	1. IDC (1) IDC 网络出口链路中断或拥塞。 (2) 由 IDC 提供服务的网站或托管主机感染病毒、木马和僵尸恶意代码，或者被利用实施网络攻击、网络仿冒等网络安全事件的情况。 (3) 通过各种渠道获得的其他信息。 2. 门户网站、搜索引擎服务提供商等 (1) 网络接入链路中断或拥塞。 (2) 系统瘫痪、遭到入侵或控制、应用服务中断等。 (3) 用户数据被篡改、丢失等。 (4) 垃圾邮件发现和处置情况。 (5) 系统感染恶意代码情况。 (6) 网页篡改、网络仿冒等情况。 (7) 通过各种渠道获得的其他信息
《工业控制系统信息安全防护指南》	第七条	七、安全监测和应急预案演练  (三) 制定工控安全事件应急响应预案，当遭受安全威胁导致工业控制系统出现异常或故障时，应立即采取紧急防护措施，防止事态扩大，并逐级报送直至属地省级工业和信息化主管部门，同时注意保护现场，以便进行调查取证
《工业控制系统信息安全事件应急管理工作指南》	第十二条	地方工业和信息化主管部门、工业企业定期将重要监测信息报国家工业信息安全发展研究中心，国家工业信息安全发展研究中心负责汇总、整理和研判，并将结果报工业和信息化部；针对可能超出本地区应对能力范围的安全风险和事件信息，及时上报，必要时工业和信息化部协调应急技术机构提供支持
	第十三条	工业和信息化部对可能影响我国工业控制系统的重大漏洞和风险，及时向有关行业、地区和工业企业发布情况通报
	第十七条	有关地方工业和信息化主管部门和工业企业应及时向工业和信息化部报告事态发展变化情况和事件处置进展情况。报告信息一般包括以下要素：事件涉及的工业控制系统名称及运营管理单位、时间、地点、原因、来源、类型、性质、危害、影响范围、发展趋势、处置措施等

续表

法律名称	法律条款	法律规定
《公共互联网网络安全威胁监测与处置办法》	第六条	<p>相关专业机构、基础电信企业、网络安全企业、互联网企业、域名注册管理和服务机构等监测发现网络安全威胁后,属于本单位自身问题的,应当立即进行处置,涉及其他主体的,应当及时将有关信息按照规定的内容要素和格式提交至工业和信息化部,以及相关省、自治区、直辖市通信管理局。</p> <p>工业和信息化部建立网络安全威胁信息共享平台,统一汇集、存储、分析、通报、发布网络安全威胁信息;制定相关接口规范,与相关单位网络安全监测平台实现对接。国家计算机网络应急技术处理协调中心负责平台建设和运行维护工作</p>
	第八条	<p>电信主管部门对专业机构的认定和处置意见进行审查后,可以对网络安全威胁采取以下一项或多项处置措施:</p> <p>(一)通知基础电信企业、互联网企业、域名注册管理和服务机构等,由其对恶意 IP 地址(或宽带接入账号)、恶意域名、恶意 URL、恶意电子邮件账号或恶意手机号码等,采取停止服务或屏蔽等措施。</p> <p>(二)通知网络服务提供者,由其清除本单位网络、系统或网站中存在的可能传播扩散的恶意程序。</p> <p>(三)通知存在漏洞、后门或已经被非法入侵、控制、篡改的网络服务和产品的提供者,由其采取整改措施,消除安全隐患;对涉及党政机关和关键信息基础设施的,同时通报其上级主管单位和网信部门。</p> <p>(四)其他可以消除、制止或控制网络安全威胁的技术措施。</p> <p>电信主管部门的处置通知应当通过书面或可验证来源的电子方式等形式送达相关单位,紧急情况下,可先电话通知,后补书面通知</p>
	第十一条	鼓励相关单位以行业自律或技术合作、技术服务等形式开展网络安全威胁监测与处置工作,并对处置行为负责,监测与处置结果应当及时报送电信主管部门
《电信网络运行监督管理办法》	第六条	<p>基础电信业务经营者总部及各级分支机构的主要负责人对本单位的网络运行维护工作负有下列职责:</p> <p>(八)及时、如实报告网络运行事故</p>
	第三十条	<p>发生网络运行事故后,基础电信业务经营者有关人员应当立即报告本单位负责人。</p> <p>单位负责人接到事故报告后,应当迅速采取有效措施,组织抢修,防止事故扩大,减少社会影响和财产损失</p>

续表

法律名称	法律条款	法律规定
《电信网络运行监督管理办法》	第三十一条	发生特别重大、重大事故后，基础电信业务经营者总部应当向工业和信息化部报告事故情况，同时其省级机构应当向相关省、自治区、直辖市通信管理局报告事故情况。 发生较大事故后，基础电信业务经营者省级机构应当向相关省、自治区、直辖市通信管理局报告事故情况。 发生一般事故后，基础电信业务经营者省级机构应当向相关省、自治区、直辖市通信管理局定期报送。 发生网络运行事故后，任何单位和个人不得迟报、漏报、谎报或瞒报
	第三十二条	网络运行事故报告分为口头报告、简要书面报告（格式见附件二）和专题书面报告（格式见附件三）三种。 发生网络运行事故后，基础电信业务经营者总部及其省级机构应当在规定时限内向电信监管部门报告（具体报告时限见附件四）
	第三十三条	基础电信业务经营者上报的简要书面报告应当经本企业主管领导或主管部门领导认定，专题书面报告须经本企业主管领导认定
	第三十四条	事故的口头报告内容应当包括事故发生时间、地点、预计影响范围、事故原因的初步判断、已经或即将采取的措施。简要书面报告的内容应当包括事故发生时间、地点、影响范围、事故原因的初步判断、事故初步处理措施等。专题书面报告的内容应当包括事故发生时间、地点、影响范围、事故原因、责任认定、处理意见、防范措施等
	第四十二条	电信监管部门应当建立网络运行情况通报制度，定期向基础电信业务经营者通报网络运行情况
	第四十四条	基础电信业务经营者有下列行为之一，电信监管部门应当予以警告并责令其限期改正。逾期未改正的，可以在行业内予以通报批评。 （八）发生网络运行事故，未及时、如实上报或者对事故调查处理不力的； （九）未按时向电信监管部门报送网络运行基础数据的

针对网络安全信息通报的法规遵从建议，表 7-6 梳理了其中涉及的技术、环境和性能等具体要求，以及网络运营者在履行网络安全信息通报义务时应当重点关注的方面。

表 7-6 网络安全信息通报的法规遵从建议

控制项	网络安全信息通报的法规遵从建议	对应条款
1. 网络安全信息通报的类型		<p>第二十五条 网络运营者应当制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险；在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告。</p> <p>第五十一条 国家建立网络安全监测预警和信息通报制度。国家网信部门应当统筹协调有关部门加强网络安全信息收集、分析和通报工作，按照规定统一发布网络安全监测预警信息。</p> <p>第五十二条 负责关键信息基础设施安全保护工作的部门，应当建立健全本行业、本领域的网络安全监测预警和信息通报制度，并按照规定报送网络安全监测预警信息</p>
组织内信息通报	<p>在网络安全事件发生后，应通知应急响应日常运行小组使其能够确定事态的严重程度和下一步将要采取的行动。在损害评估完成后，应通知应急响应领导小组。</p> <p>通知策略应定义网络安全事件发生后人员无法联络时的规程，通知规程应在应急预案中明确描述，一种通用的通知方法是呼叫树。呼叫树应包括主要的和备用的联络方法，应确定在某个人无法联系上时应采取的规程。</p> <p>需要通知的人员应在应急预案附录中的联系人清单中标明。联系人清单确定人员在其小组中的职位、姓名和联络信息（如家庭、工作电话号码、手机号码、电子邮件地址和家庭地址等）</p>	
组织外信息通报	网络安全事件发生后，组织应将相关信息及时通报给受到负面影响的外部机构、互联的单位系统及重要客户，同时根据应急响应的需要，应将相关信息准确通报给相关设备及服务提供商、电信、电力等外部组织，以获得适当的应急响应支持。对外信息通报应符合组织的对外信息发布策略	
信息上报	网络安全事件发生后，组织应按照相关规定和要求，及时将情况上报相关单位或者部门	
2. 网络安全信息通报的技术要求		
通报内容	<p>安全事件、运行状态、脆弱性与威胁和策略与配置的检测结果等实时信息</p> <p>物理环境状态、拓扑关系、日志、事件和告警信息，以及事件间的关联关系</p>	
通报形式	<p>通过统计分析图形、报表方式展示；</p> <p>通过关键字快速检索获取相关日志和流量元数据及详细信息，查询追溯事件的相关原始信息；</p> <p>通过展示攻击过程和扩散路径，进行攻击链和攻击上下文信息的呈现，多维度展示安全威胁的影响和范围</p>	
3. 网络安全信息通报的环境要求		
	组织应通过 API 的方式调用存储层的分析数据和日志数据，将数据库中每个数据项以单个图元元素表示，多种数据集构成数据图像，同时将数据的各个属性值以多维数据的形式表示，从时间、空间、地理的维度进行展示与告警	
4. 网络安全信息通报的性能要求		
	组织应确保网络安全信息通报的网络通信采用加密协议	



### 三、监督管理与法律责任

目前,我国已经建立了中央网信办、公安部牵头,工业和信息化部、国家发展改革委、国家保密局等按职责分工负责的网络安全信息通报体制机制。作为国家网络安全的主管部门,国家网信部门负责统筹协调有关部门的网络安全信息通报工作。负责关键信息基础设施安全保护工作的部门,应当建立健全本行业、本领域的网络安全信息通报制度,并按照规定报送网络安全监测预警信息。省级以上人民政府有关部门应当按照规定的权限和程序,并根据网络安全风险的特点和可能造成的危害,要求有关部门、机构和人员及时收集、报告有关信息,加强对网络安全风险的监测。在发生危害网络安全的事件时,网络运营者应当立即启动应急预案,采取相应的补救措施,并按照规定向有关主管部门报告。

法律责任方面,《网络安全法》第五十九条规定,网络运营者不履行本法第二十五条规定的网络安全保护义务,在发生危害网络安全的事件时,没有按照规定向有关主管部门报告的,由有关主管部门责令改正,给予警告;拒不改正或导致危害网络安全等后果的,处一万元以上十万元以下罚款,对直接负责的主管人员处五千元以上五万元以下罚款。

## 第四节 网络安全预警信息发布

### 一、《网络安全法》相关规定及释义

《网络安全法》第五十一条规定,国家网信部门应当按照规定统一发布网络安全监测预警信息。第五十四条第三款规定,网络安全事件发生的风险增大时,省级以上人民政府有关部门应当按照规定的权限和程序,并根据网络安全风险的特点和可能造成的危害,向社会发布网络安全风险预警,发布避免、减轻危害的措施。由此可见,《网络安全法》重点关注网络安全预警信息的发布,然而针对政府

有关部门的网络安全预警信息发布职责和网络运营者的网络安全预警信息发布义务应当予以明确。

## （一）政府有关部门的网络安全预警信息发布职责

《网络安全法》重点关注网络安全预警信息的对外发布，其中第五十一条规定，国家网信部门应当按照规定统一发布网络安全监测预警信息。第五十四条第三款规定，网络安全事件发生的风险增大时，省级以上人民政府有关部门应当按照规定的权限和程序，并根据网络安全风险的特点和可能造成的危害，向社会发布网络安全风险预警，发布避免、减轻危害的措施。由此可见，国家网信部门按照规定拥有统一面向社会发布网络安全监测预警信息的权力，而省级以上政府有关部门只有在网络安全事件发生的风险增大时，才有权根据风险评估结果，通过政府门户网站、新闻媒体、委托 CNCERT 发布等方式及时向社会发布网络安全风险预警以及避免、减轻危害的措施，以使公众及时知悉网络安全风险，采取有效的应对措施减轻网络安全风险给其带来的损害。

### 1. 国家网信部门的网络安全预警信息发布职责

具体而言，首先，国家网信部门负责网络安全风险监测通报工作，制定网络安全事件监测通报规划和方案。其核心职能之一就是作为常设的监测预警机构，及时准确地收集掌握各种情报信息，及时把握网络安全事件发生的规律和动态，有效保证对网络安全事件的性质、范围和严重程度做出准确的判断，并为接下来的应急处置奠定基础。其次，建议在国家网信部门之下应当设立网络安全风险监测中心，对网络安全风险的发生、扩散，以及影响其发生、扩散的因素进行监测；通过多种途径对国外发生、国内尚未发生的网络安全事件或国内新发生的网络安全事件，进行监测；对各行业主管部门报送的网络安全事件信息进行风险评估，及时将这些信息共享给其他存有依赖性的网络运营者、关键信息基础设施运营单位及其行业主管部门，并指导他们做出适当有效的应对措施。

### 2. 省级以上政府有关部门的网络安全预警信息发布职责

省级以上政府有关部门，包括省级以上政府网信、工信、公安、国家安全、

保密行政管理、密码管理等部门应当在网络安全事件发生的风险增大时,根据风险评估结果,通过其部门门户网站、电子公告、委托 CNCERT 发布等方式及时向社会公众发布网络安全风险预警以及避免、减轻危害的措施,以使公众及时知悉网络安全风险,采取公布的有效应对措施减轻网络安全风险给其带来的损害。另外,省级以上政府有关部门应当按照《国家网络安全事件应急预案》的要求具体落实网络安全预警信息的发布职责。

## （二）网络运营者的网络安全预警信息发布义务

《网络安全法》第五十五条规定,发生网络安全事件,要求网络运营者采取技术措施和其他必要措施,消除安全隐患,防止危害扩大,并及时向社会发布与公众有关的警示信息。针对网络运营者而言,发生网络安全事件后,负责事件处置的部门经调查评估,认为该事件对社会公众产生较大影响的,应当及时、准确、客观地向社会发布与公众有关的警示信息。一方面,发布的警示信息要统一、及时、准确,避免使社会公众产生误解;另一方面应当告知公众相关的网络安全知识,以及受事件影响的社会公众应采取的消除安全隐患、防止损害扩大的措施,维护社会公众利益。

## 二、网络安全预警信息发布的制度概述

纵观国外相关法律法规,通过建立预警机构和预警发布中心,以保障网络安全事件监测通报与预警的有效实施始终是各国在实践中的通行做法,例如,美国早期建立的国家基础设施保护中心、国家基础设施协调中心,以及近期建立的国家网络安全和通信整合中心,均为实施网络安全监测预警的国家级中心机构。新加坡国家网络威胁监测中心,用以全天候监测和分析网络威胁信息。

此外,各国基本上都建立了名为“计算机应急响应小组”(Computer Emergency Response Team, CERT)的早期预警机构,负责处理计算机安全事件和脆弱性问题,或者通过发布安全警报降低网络攻击成功的可能性。同时,在各国的早期预警机构中,计算机应急响应小组的形式多种多样,如政府机构的特别 CERT、中

小企业的 CERT、具体部门的 CERT 等。例如，日本已经建立了计算机应急响应小组协调中心（JPCERT/cc）的早期预警机构，负责处理计算机安全事件和脆弱性问题。作为日本建立的第一个计算机安全事件响应小组（Computer Security Incident Response Team, CSIRT），其组成包括网络服务提供商、安全服务/商品提供商、政府机构，以及工业和商业协会。该协调中心同时也是亚太地区计算机应急响应小组，以及事件响应和安全组论坛的成员，负责协调并结合与信息安全有关的预防措施，与其他计算机安全事件响应小组保持一致，其中有关监测预警的重要职责包括计算机安全事件响应；协调国内和国家计算机安全事件响应小组和其他相关组织的工作；促进建立新的计算机安全事件响应小组，并与其他工作小组进行合作；收集和宣传关于计算机安全事件的信息技术、缺陷和补丁、其他安全信息，并发布预警和通知；计算机安全事件的研究和分析；管理关于安全技术的研究；通过教育和培训提高信息安全意识和技能。

### 三、典型案例

国家互联网应急中心在其网站发布“关于一种蠕虫式勒索病毒的风险提示”，其中针对 WannaCry 勒索软件病毒的传播现状、影响范围、攻击特征及可采取的防范措施向社会公众做出了具体的网络安全预警信息发布。其中指出，据境内外媒体报道，一种新型的勒索病毒在全球范围内发作，在工业和信息化部指导下，其立即组织进行了研判。经研判，确实是一款新型病毒从 2017 年 5 月 12 日起在全球范围传播扩散，已影响到包括我国用户在内的多个国家的用户。该勒索病毒利用 Windows 操作系统 445 端口存在的漏洞进行传播，并具有自我复制、主动传播的特性。勒索病毒感染用户计算机后，将对计算机中的文档、图片等实施高强度加密，并向用户勒索赎金。在此提醒广大用户及时采取如下措施进行防范：①及时升级 Windows 操作系统，微软公司已发布相关补丁程序 MS17-010，可通过微软公司正规渠道进行升级；②安装并及时更新杀毒软件；③不要轻易打开来源不明的电子邮件；④及时关闭计算机、网络设备上的 445 端口；⑤定期在不同的存储介质上备份计算机上的重要文件。详细情况见《关于防范 Windows 操作系统勒索软件 WannaCry 的情况通报》。

四、网络安全预警信息发布的法规遵从框架及建议

根据《网络安全法》的有关规定，国家网信部门拥有统一面向社会发布网络安全监测预警信息的权力，省级以上政府有关部门只有在网络安全事件发生的风险增大时，才有权根据风险评估结果，通过政府门户网站、新闻媒体、委托 CNCERT 发布等方式及时向社会发布网络安全风险预警信息，以及避免、减轻危害的措施，例如，工业和信息化部通过建立网络安全威胁信息共享平台，统一发布网络安全威胁信息。在此方面，网络运营者应当重点关注以下规定及遵从建议，确保网络安全预警信息发布的及时性与统一性。

网络安全预警信息发布的法规遵从框架如表 7-7 所示。

表 7-7 网络安全预警信息发布的法规遵从框架

法律名称	法律条款	法律规定
《网络安全法》	第五十一条	国家建立网络安全监测预警和信息通报制度。国家网信部门应当统筹协调有关部门加强网络安全信息收集、分析和通报工作，按照规定统一发布网络安全监测预警信息
	第五十四条	网络安全事件发生的风险增大时，省级以上人民政府有关部门应当按照规定的权限和程序，并根据网络安全风险的特点和可能造成的危害，采取下列措施：  (三) 向社会发布网络安全风险预警，发布避免、减轻危害的措施
	第五十五条	发生网络安全事件，应当立即启动网络安全事件应急预案，对网络安全事件进行调查和评估，要求网络运营者采取技术措施和其他必要措施，消除安全隐患，防止危害扩大，并及时向社会发布与公众有关的警示信息
《关键信息基础设施安全保护条例（征求意见稿）》	第三十六条	国家网信部门统筹建立关键信息基础设施网络安全监测预警体系和信息通报制度，组织指导有关机构开展网络安全信息汇总、分析研判和通报工作，按照规定统一发布网络安全监测预警信息
《计算机信息系统安全保护条例》	第二十条	违反本条例的规定，有下列行为之一的，由公安机关处以警告或停机整顿：  (三) 不按照规定时间报告计算机信息系统中发生的案件的
《公共互联网网络安全威胁监测与处置办法》	第六条	工业和信息化部建立网络安全威胁信息共享平台，统一汇集、存储、分析、通报、发布网络安全威胁信息；制定相关接口规范，与相关单位网络安全监测平台实现对接。国家计算机网络应急技术处理协调中心负责平台建设和运行维护工作

针对网络安全预警信息发布的法规遵从建议，表 7-8 梳理了其中涉及的技术和环境等具体要求，以及网络运营者在履行网络安全预警信息发布义务时应当重点关注的几个方面。

表 7-8 网络安全预警信息发布的法规遵从建议

控制项	网络安全预警信息发布的法规遵从建议	对应条款
1. 网络安全预警信息发布的技术要求		第五十一条 国家建立网络安全监测预警和信息通报制度。国家网信部门应当统筹协调有关部门加强网络安全信息收集、分析和通报工作，按照规定统一发布网络安全监测预警信息。
安全事件分类	根据设备用途分为网络设备、安全设备、主机系统、数据库系统、应用程序、网管系统和日志服务器等； 根据事件产生原因分为漏洞、病毒/木马、可疑活动、扫描探测、拒绝服务类、认证/授权/访问类等	
安全事件分级	组织应根据原始事件的原始等级，重定义定级对应为“很低、低、中等、高、很高”	
发布方式	保存预警信息直接进行展示、统计和分析； 通过网络协议等方式发送预警信息供第三方系统分析和处理； 高级别预警信息发布应支持短信、即时通信等信息推送方式，也应支持声音、闪光等强制通知方式； 预警信息发布响应动作应支持设备联动，包括对其他设备执行命令脚本、命令行等	第五十四条 网络安全事件发生的风险增大时，省级以上人民政府有关部门应当按照规定的权限和程序，并根据网络安全风险的特点和可能造成的危害，采取下列措施：  (三) 向社会发布网络安全风险预警，发布避免、减轻危害的措施。
发布要求	网络安全事件发生后，根据网络安全事件的严重程度，组织应指定特定的小组及时向新闻媒体发布相关信息，指定的小组应严格按照组织相关规定和要求对外发布信息，同时组织内其他部门或个人不得随意接受新闻媒体采访或对外发表自己的看法	第五十五条 发生网络安全事件，应当立即启动网络安全事件应急预案，对网络安全事件进行调查和评估，要求网络运营者采取技术措施和其他必要措施，消除安全隐患，防止危害扩大，并及时向社会发布与公众有关的警示信息
2. 网络安全预警信息发布的环境要求		
	组织应通过 API 的方式调用存储层的分析数据和日志数据，将数据库中每个数据项以单个图元元素表示，多种数据集构成数据图像，同时将数据的各个属性值以多维数据的形式表示，从时间、空间、地理的维度进行预警信息发布	

## 五、监督管理与法律责任

《网络安全法》第八条第一款规定，国家网信部门负责统筹协调网络安全工作和相关监督管理工作。具体而言，为了协调网络信息通报工作的协同性和一致性，

《网络安全法》第五十一条规定，国家网信部门应当统筹协调有关部门加强网络安全信息收集、分析和通报工作，按照规定统一发布网络安全监测预警信息。具体而言，国家网信部门负责网络安全监测预警信息的统一对外发布工作，能够保证预警信息发布的准确性、可信性及统一性。

## 第五节 网络安全事件应急预案

### 一、《网络安全法》相关规定及释义

《网络安全法》第二十五条规定，网络运营者应当制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险；在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告。《网络安全法》第五十三条规定，国家网信部门协调有关部门建立健全网络安全风险评估和应急工作机制，制定网络安全事件应急预案，并定期组织演练。负责关键信息基础设施安全保护工作的部门应当制定本行业、本领域的网络安全事件应急预案，并定期组织演练。网络安全事件应急预案应当按照事件发生后的危害程度、影响范围等因素对网络安全事件进行分级，并规定相应的应急处置措施。

应急预案是指为依法、迅速、科学、有序应对突发事件，最大限度减少突发事件及其造成的损害而预先制定的工作方案。应急预案作为一种事前预防措施，可以最大限度地预防和减少网络安全事件及其造成的损害，维护国家和社会稳定，保障公民合法权益免受侵犯。我国2013年公布的《突发事件应急预案管理办法》已有对突发事件应对的具体规则，其中确立了应急预案管理遵循统一规划、分类指导、分级负责、动态管理的原则。网络安全事件作为社会突发事件的一种，其应急预案管理也应遵循上述原则。在实践中，应加强应急预案的制定、审批、备案、公布、演练、修订和保障工作，充分发挥网络安全应急预案的重要作用。

## （一）网络安全应急预案的制定

根据我国《网络安全法》第五十三条的规定，国家网信部门协调有关部门制定本行业、本领域的网络安全事件应急预案，负责关键信息基础设施安全保护工作的部门应当制定本行业、本领域的网络安全事件应急预案。同时，《网络安全法》第二十五条规定，网络运营者应当制定网络安全事件应急预案。第三十四条第四款规定，关键信息基础设施的运营者应当制定网络安全事件应急预案，并定期进行演练。

2017 年 1 月，中央网信办印发了《国家网络安全事件应急预案》，这是落实《网络安全法》有关制定网络安全事件应急预案的重要举措。《国家网络安全事件应急预案》分为总则、组织机构与职责、监测与预警、应急处置、调查与评估、预防工作、保障措施、附则八个部分，全面系统地规定了应对网络安全事件的具体措施，为工信部、公安部、国家保密局等政府有关部门遵从《网络安全法》的相关规定提供了更具有可操作性的实施指引。

《国家网络安全事件应急预案》是国家层面针对网络安全事件适用的综合应急预案。除此以外，负责关键信息基础设施安全保护工作的部门也应当落实《网络安全法》的规定，制定本行业、本领域的网络安全事件应急预案，这些预案应当紧密结合本行业、本企业的实际情况，做出具有针对性、可操作性的安排。目前，已有政府有关部门制定了本行业、本领域的网络安全应急预案，例如，《银行业重要信息系统突发事件应急管理规范（试行）》、《证券期货业网络与网络安全事件应急预案》、《公共互联网网络安全应急预案》等。此外，地方政府及相关部门也制定了相关应急预案，例如，山东保监局 2015 年制定了《山东保险业网络与网络安全突发事件应急预案》。实践中，有的行业或地方也制定了本行业或该区域的网络安全事件应急预案，但并未向社会公开。

《网络安全法》正式施行后，政府有关部门、行业主管或监管部门、网络运营者都应当按照《网络安全法》的规定制定其行业内部、组织内部或本单位的网络安全事件应急预案，有必要出台网络安全事件应急预案管理办法，规范应急预案的制定工作，提高应急预案的科学性、合理性和可操作性。值得注意的是，编制应急预案应当在开展风险评估和应急资源调查的基础上进行。

实践中，各类应急预案的内容重合导致网络安全事件发生后相关主体疲于应



对。例如，企业内部发生网络安全事件后，可能同时触发《国家突发公共事件总体应急预案》、《国家网络安全事件应急预案》、《关键信息基础设施的行业网络安全事件应急预案》、《安全生产应急预案》等，由此将涉及多个主管单位的介入，如果让企业分别向多个部门汇报情况、接受多头指挥，会导致企业在应对网络安全事件时无所适从。因此，在制定应急预案时应当充分考虑这一情况，相关部门在执行预案时也应当注意协调。

## （二）网络安全事件的分类分级

我国《网络安全法》第五十三条第三款规定，网络安全事件应急预案应当按照事件发生后的危害程度、影响范围等因素对网络安全事件进行分级，并规定相应的应急处置措施。网络安全事件所造成的危害程度，小到针对个人用户的账户或密码篡改，导致窃取敏感信息等非法利益，大到针对国家关键信息基础设施，导致国家安全和社会稳定受到威胁，整个社会无法正常持续运行。基于此，应当根据网络安全事件的不同危害程度和影响范围，对网络安全事件进行分级分类管理，有的放矢地加以应对，从而在保障国家、社会和个人利益不受非法侵害的同时提高应急资源的利用效率，实现网络安全的经济可持续发展。

### 1. 网络安全事件的分类

《国家网络安全事件应急预案》规定，网络安全事件是指由于人为因素、软硬件缺陷或故障、自然灾害等，对网络和信息系统或其中的数据造成危害，对社会造成负面影响的事件。根据 2007 年《网络安全事件分类分级指南》（GB/Z 20986—2007），网络安全事件可以分为七类。

（1）有害程序事件，是指蓄意制造、传播有害程序，或者因受到有害程序的影响而导致的网络安全事件，包括计算机病毒事件、蠕虫事件、特洛伊木马事件、僵尸网络事件、混合攻击程序事件、网页内嵌恶意代码事件和其他有害程序事件等。

（2）网络攻击事件，是指通过网络或其他技术手段，利用信息系统的配置缺陷、协议缺陷、程序缺陷或使用暴力手段对信息系统实施攻击，并造成信息系统异常或对信息系统当前运行造成潜在危害的网络安全事件，包括拒绝服务攻击事件、后门攻击事件、漏洞攻击事件、网络扫描窃听事件、网络钓鱼事件、干扰事件和其他网络攻击事件等。

(3) 信息破坏事件，是指通过网络或其他技术手段，造成信息系统中的信息被篡改、假冒、泄露、窃取等而导致的网络安全事件，包括信息篡改事件、信息假冒事件、信息泄露事件、信息窃取事件、信息丢失事件和其他信息破坏事件等。

(4) 信息内容安全事件，是指利用信息网络发布、传播危害国家安全、社会稳定和公共利益内容的网络安全事件，包括违反宪法和法律、行政法规的网络安全事件；针对社会事项进行讨论、评论，形成网上敏感的舆论热点，出现一定规模炒作的网络安全事件；组织串联、煽动集会游行的网络安全事件；其他信息内容安全事件。

(5) 设备设施故障，是指由于信息系统自身故障或外围保障措施故障而导致的网络安全事件，以及人为地使用非技术手段有意或无意地造成信息系统破坏而导致的网络安全事件，包括软硬件自身故障、外围保障设施故障、人为破坏事故和其他设备设施故障。

(6) 灾害性事件，是指由于不可抗力对网络和信息系统的物理破坏而导致的网络安全事件，包括水灾、雪灾、台风、地震、雷击、坍塌、火灾、恐怖袭击、战争等导致的网络安全事件。

(7) 其他事件，是指不能归为以上六个基本分类的网络安全事件。

## 2. 网络安全事件的分级

《网络安全事件分类分级指南》对网络安全事件的分级主要基于三个要素的考虑：①信息系统的重要程度，主要考虑信息系统所承载的业务对国家安全、经济建设、社会生活的重要性及业务对信息系统的依赖程度，划分为特别重要信息系统、重要信息系统和一般信息系统；②系统损失，是指由于网络安全事件对信息系统的软硬件、功能及数据的破坏，导致系统业务中断，从而给事发组织所造成的损失，其大小主要考虑恢复系统正常运行和消除安全事件负面影响所需付出的代价，划分为特别严重的系统损失、严重的系统损失、较大的系统损失和较小的系统损失；③社会影响，是指网络安全事件对社会造成影响的范围和程度，其大小主要考虑国家安全、社会秩序、经济建设和公众利益等方面的影响，划分为特别重大的社会影响、重大的社会影响、较大的社会影响和一般的社会影响。

根据网络安全事件的分级考虑要素，将网络安全事件划分为四个级别，即特别重大事件、重大事件、较大事件和一般事件。

(1) 特别重大事件（I级），是指能够导致特别严重影响或破坏的网络安全事件，包括会使特别重要信息系统遭受特别严重的系统损失或产生特别重大的社会影响。

(2) 重大事件（II级），是指能够导致严重影响或破坏的网络安全事件，包括以下情况：会使特别重要信息系统遭受严重的系统损失或使重要信息系统遭受特别严重的系统损失；产生重大的社会影响。

(3) 较大事件（III级），是指能够导致较严重影响或破坏的网络安全事件，包括以下情况：会使特别重要信息系统遭受较大的系统损失或使重要信息系统遭受严重的系统损失、一般信息系统遭受特别严重的系统损失；产生较大的社会影响。

(4) 一般事件（IV级），是指不满足以上条件的网络安全事件，包括以下情况：会使特别重要信息系统遭受较小的系统损失或使重要信息系统遭受较大的系统损失，一般信息系统遭受严重或严重以下级别的系统损失；产生一般的社会影响。

值得注意的是，《国家网络安全事件应急预案》在《网络安全事件分类分级指南》的基础上，将网络安全事件分为四级：特别重大网络安全事件、重大网络安全事件、较大网络安全事件、一般网络安全事件。

(1) 符合下列情形之一的，为特别重大网络安全事件：①重要网络和信息系統遭受特别严重的系统损失，造成系统大面积瘫痪，丧失业务处理能力；②国家秘密信息、重要敏感信息和关键数据丢失或被窃取、篡改、假冒，对国家安全和社会稳定构成特别严重威胁；③其他对国家安全、社会秩序、经济建设和公众利益构成特别严重威胁、造成特别严重影响的网络安全事件。

(2) 符合下列情形之一且未达到特别重大网络安全事件的，为重大网络安全事件：①重要网络和信息系統遭受严重的系统损失，造成系统长时间中断或局部瘫痪，业务处理能力受到极大影响；②国家秘密信息、重要敏感信息和关键数据丢失或被窃取、篡改、假冒，对国家安全和社会稳定构成严重威胁；③其他对国家安全、社会秩序、经济建设和公众利益构成严重威胁、造成严重影响的网络安全事件。

(3) 符合下列情形之一且未达到重大网络安全事件的，为较大网络安全事件：①重要网络和信息系統遭受较大的系统损失，造成系统中断，明显影响系统效率，

业务处理能力受到影响；②国家秘密信息、重要敏感信息和关键数据丢失或被窃取、篡改、假冒，对国家安全和社会稳定构成较严重威胁；③其他对国家安全、社会秩序、经济建设和公众利益构成较严重威胁、造成较严重影响的网络安全事件。

（4）除上述情形外，对国家安全、社会秩序、经济建设和公众利益构成一定威胁、造成一定影响的网络安全事件，为一般网络安全事件。

### （三）网络安全事件应急预案的内容

网络安全事件应急预案的内容具体包括：①网络安全事件应急管理的方针、政策和工作原则；②网络安全应急响应责任人、组织机构及其职责；③采取的应急行动、处置程序、应急保障措施、可调用或可请求援助的应急资源情况及如何实施等；④应急人员沟通与协调方式；⑤事后恢复与重建措施；⑥明确应急恢复过程中的关键状态及其沟通报告内容等。值得注意的是，制定网络安全事件应急预案还应当考虑业务的分类、业务风险的等级划分、技术现状分析、突发事件归类分析，还应充分考虑突发事件的重点部分，优先考虑对社会、用户和内部经营管理影响最大的事件。应急预案应当涵盖业务应急措施、技术应急措施和风险应急措施，并随着过程、环境的变换而不断更新。此外，政府及其部门、有关单位和基层组织可结合本地区、本部门和本单位具体情况，编制应急预案操作手册，内容一般包括风险隐患分析、处置工作程序、响应措施、应急队伍和装备物资情况，以及相关单位联络人员和电话等。

## 二、网络安全事件应急预案的法规遵从框架及建议

网络安全事件应急预案的制定应当依据有关法律、行政法规和制度，侧重明确应急响应责任人、风险隐患监测、信息报告、预警响应、应急处置、可调用或可请求援助的应急资源情况及如何实施等。作为大型企业集团的网络运营者可根据相关标准规范和实际工作需要，参照国际惯例，建立本集团的网络安全事件应急预案体系。编制网络安全事件应急预案应当在开展网络安全风险评估和应急资源调查的基础上进行。

网络安全事件应急预案的法规遵从框架如表 7-9 所示。

表 7-9 网络安全事件应急预案的法规遵从框架

法律名称	法律条款	法律规定
《网络安全法》	第二十五条	网络运营者应当制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险；在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告
	第三十四条	除本法第二十一条的规定外，关键信息基础设施的运营者还应当履行下列安全保护义务： （四）制定网络安全事件应急预案，并定期进行演练
	第五十三条	国家网信部门协调有关部门建立健全网络安全风险评估和应急工作机制，制定网络安全事件应急预案，并定期组织演练。 负责关键信息基础设施安全保护工作的部门应当制定本行业、本领域的网络安全事件应急预案，并定期组织演练。 网络安全事件应急预案应当按照事件发生后的危害程度、影响范围等因素对网络安全事件进行分级，并规定相应的应急处置措施
	第五十五条	发生网络安全事件，应当立即启动网络安全事件应急预案，对网络安全事件进行调查和评估，要求网络运营者采取技术措施和其他必要措施，消除安全隐患，防止危害扩大，并及时向社会发布与公众有关的警示信息
《突发事件应急预案管理办法》	第五条	应急预案编制要依据有关法律、行政法规和制度，紧密结合实际，合理确定内容，切实提高针对性、实用性和可操作性
	第九条	单位和基层组织应急预案由机关、企业、事业单位、社会团体和居委会、村委会等法人和基层组织制定，侧重明确应急响应责任人、风险隐患监测、信息报告、预警响应、应急处置、人员疏散撤离组织和路线、可调用或可请求援助的应急资源情况及如何实施等，体现自救互救、信息报告和先期处置特点。 大型企业集团可根据相关标准规范和实际工作需要，参照国际惯例，建立本集团应急预案体系
	第十条	政府及其部门、有关单位和基层组织可根据应急预案，并针对突发事件现场处置工作灵活制定现场工作方案，侧重明确现场组织指挥机制、应急队伍分工、不同情况下的应对措施、应急装备保障和自我保障等内容
	第十一条	政府及其部门、有关单位和基层组织可结合本地区、本部门和本单位具体情况，编制应急预案操作手册，内容一般包括风险隐患分析、处置工作程序、响应措施、应急队伍和装备物资情况，以及相关单位联络人员和电话等
	第十二条	对预案应急响应是否分级、如何分级、如何界定分级响应措施等，由预案制定单位根据本地区、本部门和本单位的实际情况确定
	第十四条	应急预案编制部门和单位应组成预案编制工作小组，吸收预案涉及主要部门和单位业务相关人员、有关专家及有现场处置经验的人员参加。编制工作小组组长由应急预案编制部门或单位有关负责人担任

续表

法律名称	法律条款	法律规定
《突发事件应急预案管理办法》	第十五条	编制应急预案应当在开展风险评估和应急资源调查的基础上进行。 (一) 风险评估。针对突发事件特点, 识别事件的危害因素, 分析事件可能产生的直接后果, 以及次生、衍生后果, 评估各种后果的危害程度, 提出控制风险、治理隐患的措施。 (二) 应急资源调查。全面调查本地区、本单位第一时间可调用的应急队伍、装备、物资、场所等应急资源状况和合作区域内可请求援助的应急资源状况, 必要时对本地居民应急资源情况进行调查, 为制定应急响应措施提供依据
	第十六条	单位和基层组织应急预案编制过程中, 应根据法律、行政法规要求或实际需要, 征求相关公民、法人或其他组织的意见
	第十九条	单位和基层组织应急预案须经本单位或基层组织主要负责人或分管负责人签发, 审批方式根据实际情况确定
	第二十四条	应急预案编制单位应当建立定期评估制度, 分析评价预案内容的针对性、实用性和可操作性, 实现应急预案的动态优化和科学规范管理
	第二十五条	有下列情形之一的, 应当及时修订应急预案: (一) 有关法律、行政法规、规章、标准、上位预案中的有关规定发生变化的; (二) 应急指挥机构及其职责发生重大调整的; (三) 面临的风险发生重大变化的; (四) 重要应急资源发生重大变化的; (五) 预案中的其他重要信息发生变化的; (六) 在突发事件实际应对和应急演练中发现问题需要做出重大调整的; (七) 应急预案制定单位认为应当修订的其他情况
	第二十六条	应急预案修订涉及组织指挥体系与职责、应急处置程序、主要处置措施、突发事件分级标准等重要内容的, 修订工作应参照本办法规定的预案编制、审批、备案、公布程序组织进行。仅涉及其他内容的, 修订程序可根据情况适当简化
	第二十八条	应急预案编制单位应当通过编发培训材料、举办培训班、开展工作研讨等方式, 对与应急预案实施密切相关的管理人员和专业救援人员等组织开展应急预案培训
《关键信息基础设施安全保护条例(征求意见稿)》	第二十四条	除本条例第二十三条外, 运营者还应当按照国家法律法规的规定和相关国家标准的强制性要求, 履行下列安全保护义务: (四) 制定网络安全事件应急预案并定期进行演练
	第三十九条	国家行业主管或监管部门应当组织制定本行业、本领域的网络安全事件应急预案, 并定期组织演练, 提升网络安全事件应对和灾难恢复能力。发生重大网络安全事件或接到网信部门的预警信息后, 应立即启动应急预案组织应对, 并及时报告有关情况

续表

法律名称	法律条款	法律规定
《国家网络安全事件应急预案》	1.4 事件分级	<p>网络安全事件分为四级：特别重大网络安全事件、重大网络安全事件、较大网络安全事件、一般网络安全事件。</p> <p>（1）符合下列情形之一的，为特别重大网络安全事件：</p> <p>①重要网络和信息系統遭受特別严重的系統损失，造成系統大面积瘫痪，丧失业务处理能力。</p> <p>②国家秘密信息、重要敏感信息和关键数据丢失或被窃取、篡改、假冒，对国家安全和社会稳定构成特别严重威胁。</p> <p>③其他对国家安全、社会秩序、经济建设和公众利益构成特别严重威胁、造成特别严重影响的网络安全事件。</p> <p>（2）符合下列情形之一且未达到特别重大网络安全事件的，为重大网络安全事件：</p> <p>①重要网络和信息系統遭受严重的系統损失，造成系統长时间中断或局部瘫痪，业务处理能力受到极大影响。</p> <p>②国家秘密信息、重要敏感信息和关键数据丢失或被窃取、篡改、假冒，对国家安全和社会稳定构成严重威胁。</p> <p>③其他对国家安全、社会秩序、经济建设和公众利益构成严重威胁、造成严重影响的网络安全事件。</p> <p>（3）符合下列情形之一且未达到重大网络安全事件的，为较大网络安全事件：</p> <p>①重要网络和信息系統遭受较大的系統损失，造成系統中断，明显影响系統效率，业务处理能力受到影响。</p> <p>②国家秘密信息、重要敏感信息和关键数据丢失或被窃取、篡改、假冒，对国家安全和社会稳定构成较严重威胁。</p> <p>③其他对国家安全、社会秩序、经济建设和公众利益构成较严重威胁、造成较严重影响的网络安全事件。</p> <p>（4）除上述情形外，对国家安全、社会秩序、经济建设和公众利益构成一定威胁、造成一定影响的网络安全事件，为一般网络安全事件。</p>
	附件 1 网络安全事件分类	<p>网络安全事件分为有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障、灾害性事件和其他网络安全事件等。</p> <p>（1）有害程序事件分为计算机病毒事件、蠕虫事件、特洛伊木马事件、僵尸网络事件、混合程序攻击事件、网页内嵌恶意代码事件和其他有害程序事件。</p> <p>（2）网络攻击事件分为拒绝服务攻击事件、后门攻击事件、漏洞攻击事件、网络扫描窃听事件、网络钓鱼事件、干扰事件和其他网络攻击事件。</p> <p>（3）信息破坏事件分为信息篡改事件、信息假冒事件、信息泄露事件、信息窃取事件、信息丢失事件和其他信息破坏事件。</p>

续表

法律名称	法律条款	法律规定
《国家网络安全事件应急预案》	附件 1 网络安全事件分类	<p>(4) 信息内容安全事件是指通过网络传播法律法规禁止信息,组织非法串联、煽动集会游行或炒作敏感问题并危害国家安全、社会稳定和公共利益的事件。</p> <p>(5) 设备设施故障分为软硬件自身故障、外围保障设施故障、人为破坏事故和其他设备设施故障。</p> <p>(6) 灾害性事件是指由自然灾害等其他突发事件导致的网络安全事件。</p> <p>(7) 其他事件是指不能归为以上分类的网络安全事件</p>
	8.1 预案管理	<p>本预案原则上每年评估一次,根据实际情况适时修订。修订工作由中央网信办负责。</p> <p>各省(区、市)、各部门、各单位要根据本预案制定或修订本地区、本部门、本行业、本单位网络安全事件应急预案</p>
《银行业重要信息系统突发事件应急管理规范(试行)》	第十九条	银行业金融机构应根据恢复时间目标和恢复点目标,结合风险控制策略,从基础设施、网络、信息系统等不同方面,分类制定本机构应急预案
	第二十条	<p>银行业金融机构编制的信息系统应急预案应包括以下内容:</p> <p>(一) 明确有关各方的分工和责任;</p> <p>(二) 说明重要信息系统的业务影响范围、恢复时间目标、恢复点目标,以及信息系统包括的系统资源,明确资源的物理位置、设备型号、软件资源、网络配置等关键信息;</p> <p>(三) 明确各类故障的诊断方法和流程,应急场景应至少覆盖电力故障、火情水灾、治安、病毒爆发、网络攻击、人为破坏、不可抗力、计算机硬件故障、操作系统故障、系统漏洞、应用系统故障,以及其他各类与信息系统相关的故障;</p> <p>(四) 制定系统恢复流程和应急处置操作手册,尽可能将操作代码化、自动化,降低应急处置过程中产生的操作风险;</p> <p>(五) 明确应急恢复过程中的关键状态,并明确不同状态的沟通和报告内容及等级;</p> <p>(六) 明确应急相关人员的协调内容和沟通方式;</p> <p>(七) 明确系统重建步骤,确保信息系统恢复正常业务处理能力</p>
	第二十一条	银行业金融机构应将支撑信息系统运行的重要外包服务的应急管理纳入其中,建立重要外包服务的专项应急预案,对于重要基础设施、重要设备、网络、系统集成,以及其他外包服务商的技术与产品政策、服务水平、服务能力制定风险应对措施,外包服务的应急预案应能够保障银行业信息系统恢复时间目标和恢复点目标的要求
	第二十三条	当信息系统发生系统上线、系统升级、网络改造、设备更新、配置参数调整等变更时应及时更新应急预案,并适时实施演练



续表

法律名称	法律条款	法律规定
《工业控制系统信息安全事件应急管理工作指南》	第五条	工业和信息化部指导地方工业和信息化主管部门、应急技术机构、工业企业做好工控安全应急管理工作
	第六条	地方工业和信息化主管部门负责指导本地区工控安全应急管理工作
	第七条	工控安全应急技术机构负责具体开展工控安全风险监测、态势研判、威胁预警、事件处置等工作
	第八条	工业企业负有工控安全主体责任，应建立健全工控安全责任制，负责本单位工控安全应急管理工作，落实人财物保障
	第九条	工业和信息化部指导地方工业和信息化主管部门、应急技术机构、工业企业等建立工控安全联络员机制，指定工控安全应急工作联络员，报工业和信息化部备案，联络员和联络方式发生变化时需及时报工业和信息化部。工业和信息化部根据工作需要组织召开联络员会议
	第十条	地方工业和信息化主管部门指导本地区应急技术机构、工业企业建立工控安全应急值守机制，实行领导带班、专人值守工作制度，做好工控安全风险、威胁、事件信息日常监测和报告工作。应急响应状态下，实行“7×24”小时值守，加强信息监测、收集与研判，做好信息跟踪报告
	第十四条	在国家重要活动、会议等敏感时期，工业和信息化部指导地方工业和信息化主管部门、应急技术机构、工业企业开展工控安全事件预防和应急管理工作
	第十五条	地方工业和信息化主管部门、工业企业加强工控安全监测和风险研判，对可能造成重大影响的风险和事件信息应及时上报，必要时实行 24 小时零报告制度。重点单位、重要部位实施 24 小时值守，保持通信联络畅通。相关工业企业应加强对工业控制系统的巡检巡查，原则上不在敏感时期对工业控制系统进行调整或升级
	第十六条	对于可能发生或已经发生的工控安全事件，工业企业应立即开展应急处置，采取科学有效方法及时施救，力争将损失降到最小，尽快恢复受损工业控制系统的正常运行。当事发工业企业应急处置力量不足时，可请求上级主管部门协调应急技术机构提供支援
	第十八条	工业和信息化部指导、督促事发企业开展应急处置工作，必要时派出工作组赴现场指挥协调应急处置工作，协调应急技术机构提供技术支援
	第十九条	应急处置结束、系统恢复运行后，相关工业企业要尽快消除事件造成的不良影响，做好事件分析总结工作，总结报告应在 30 天内以书面形式报工业和信息化部
	第二十条	对于工控安全事件性质、起因、范围、损失等，工业和信息化主管部门和相关人员应做好舆论宣传和引导工作

续表

法律名称	法律条款	法律规定
《工业控制系统信息安全防护指南》	第七条	制定工控安全事件应急响应预案,当遭受安全威胁导致工业控制系统出现异常或故障时,应立即采取紧急防护措施,防止事态扩大,并逐级报送直至属地省级工业和信息化主管部门,同时注意保护现场,以便进行调查取证
	第七条	定期对工业控制系统的应急响应预案进行演练,必要时对应急响应预案进行修订
《电信网络运行监督管理办法》	第六条	基础电信业务经营者总部及各级分支机构的主要负责人对本单位的网络运行维护工作负有下列职责: (六) 组织制定并实施本单位的网络运行事故应急处置预案
	第四十四条	基础电信业务经营者有下列行为之一,电信监管部门应当予以警告并责令其限期改正。逾期未改正的,可以在行业内予以通报批评。 (三) 未制定和演练网络运行事故应急处置预案的

针对网络安全事件应急预案制定的法规遵从建议,表 7-10 重点梳理了网络安全事件应急预案制定过程中涉及的有关网络安全事件分类分级情况,以及网络安全事件应急响应组织、应急响应流程、分类应急处置措施的具体要求。

表 7-10 网络安全事件应急预案制定的法规遵从建议

控制项	网络安全事件应急预案制定的法规遵从建议	对应条款
1. 网络安全事件分类分级		第二十五条 网络运营者应当制定网络安全事件应急预案,及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险;在发生危害网络安全的事件时,立即启动应急预案,采取相应的补救措施,并按照规定向有关主管部门报告。
网络安全事件分级	网络安全事件分为四级:特别重大网络安全事件、重大网络安全事件、较大网络安全事件、一般网络安全事件。  (1) 符合下列情形之一的,为特别重大网络安全事件。  ①重要网络和信息系统遭受特别严重的系统损失,造成系统大面积瘫痪,丧失业务处理能力。  ②国家秘密信息、重要敏感信息和关键数据丢失或被窃取、篡改、假冒,对国家安全和社会稳定构成特别严重威胁。  ③其他对国家安全、社会秩序、经济建设和公众利益构成特别严重威胁、造成特别严重影响的网络安全事件。	第三十四条 除本法第二十一条的规定外,关键信息基础设施的运营者还应当履行下列安全保护义务:  (四)制定网络安全事件应急预案,并定期进行演练。
		第五十三条 国家网信部门协调有关部门建立健全网络安全风险评估和应急工作机制,制定网络安全事件应急预案,并定期组

续表

控制项	网络安全事件应急预案制定的法规遵从建议	对应条款
网络安全事件分级	<p>（2）符合下列情形之一且未达到特别重大网络安全事件的，为重大网络安全事件。</p> <p>①重要网络和信息系统遭受严重的系统损失，造成系统长时间中断或局部瘫痪，业务处理能力受到极大影响。</p> <p>②国家秘密信息、重要敏感信息和关键数据丢失或被窃取、篡改、假冒，对国家安全和社会稳定构成严重威胁。</p> <p>③其他对国家安全、社会秩序、经济建设和公众利益构成严重威胁、造成严重影响的网络安全事件。</p> <p>（3）符合下列情形之一且未达到重大网络安全事件的，为较大网络安全事件。</p> <p>①重要网络和信息系统遭受较大的系统损失，造成系统中断，明显影响系统效率，业务处理能力受到影响。</p> <p>②国家秘密信息、重要敏感信息和关键数据丢失或被窃取、篡改、假冒，对国家安全和社会稳定构成较严重威胁。</p> <p>③其他对国家安全、社会秩序、经济建设和公众利益构成较严重威胁、造成较严重影响的网络安全事件。</p> <p>（4）除上述情形外，对国家安全、社会秩序、经济建设和公众利益构成一定威胁、造成一定影响的网络安全事件，为一般网络安全事件</p>	<p>织演练。</p> <p>负责关键信息基础设施安全保护工作的部门应当制定本行业、本领域的网络安全事件应急预案，并定期组织演练。</p> <p>网络安全事件应急预案应当按照事件发生后的危害程度、影响范围等因素对网络安全事件进行分级，并规定相应的应急处置措施。</p> <p>第五十五条 发生网络安全事件，应当立即启动网络安全事件应急预案，对网络安全事件进行调查和评估，要求网络运营者采取技术措施和其他必要措施，消除安全隐患，防止危害扩大，并及时向社会发布与公众有关的警示信息</p>
网络安全事件分类	<p>网络安全事件分为有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障、灾害性事件和其他网络安全事件等。</p> <p>（1）有害程序事件分为计算机病毒事件、蠕虫事件、特洛伊木马事件、僵尸网络事件、混合程序攻击事件、网页内嵌恶意代码事件和其他有害程序事件。</p>	

续表

控制项	网络安全事件应急预案制定的法规遵从建议	对应条款
网络安全事件分类	<p>(2) 网络攻击事件分为拒绝服务攻击事件、后门攻击事件、漏洞攻击事件、网络扫描窃听事件、网络钓鱼事件、干扰事件和其他网络攻击事件。</p> <p>(3) 信息破坏事件分为信息篡改事件、信息假冒事件、信息泄露事件、信息窃取事件、信息丢失事件和其他信息破坏事件。</p> <p>(4) 信息内容安全事件是指通过网络传播法律法规禁止信息，组织非法串联、煽动集会游行或炒作敏感问题并危害国家安全、社会稳定和公众利益的事件。</p> <p>(5) 设备设施故障分为软硬件自身故障、外围保障设施故障、人为破坏事故和其他设备设施故障。</p> <p>(6) 灾害性事件是指由自然灾害等其他突发事件导致的网络安全事件。</p> <p>(7) 其他事件是指不能归为以上分类的网络安全事件</p>	
2. 网络安全事件应急响应组织		
应急响应领导小组	<p>应急响应领导小组是网络安全应急响应工作的组织领导机构，组长应由组织最高管理层成员担任。领导小组的职责是领导和决策网络安全应急响应的重大事宜，主要包括：</p> <p>对应急响应工作的承诺和支持，包括发布正式文件、提供必要资源（人财物）等；</p> <p>审核并批准应急响应策略；</p> <p>审核并批准应急预案；</p> <p>批准和监督应急预案的执行；</p> <p>启动定期评审、修订应急预案；</p> <p>负责组织的外部协作工作</p>	

续表

控制项	网络安全事件应急预案制定的法规遵从建议	对应条款
应急响应技术保障小组	应急响应技术保障小组的主要职责包括： 制定网络安全事件技术应对表； 制定网络安全事件区域技术应对表； 制定具体角色和职责分工细则； 制定应急响应协同调度方案； 考察和管理相关技术基础	
应急响应专家小组	应急响应专家小组的主要职责包括： 对重大网络安全事件进行评估，提出启动应急响应级别的建议； 研究分析网络安全事件的相关情况及发展趋势，为应急响应提供咨询或提出建议； 分析网络安全事件原因及造成的危害，为应急响应提供技术支持	
应急响应实施小组	应急响应实施小组的主要职责包括： 分析应急响应需求（如风险评估、业务影响分析等）； 确定应急响应策略和等级； 实现应急响应策略； 编制应急预案文档； 实施应急预案； 组织应急预案的测试、培训和演练； 合理部署和使用应急响应资源； 总结应急响应工作，提交应急响应总结报告； 执行应急预案的评审、修订任务	
应急响应日常运行小组	应急响应日常运行小组的主要职责包括： 协助灾难恢复系统实施； 备份中心日常管理； 备份系统的运行和维护； 应急监控系统的运作和维护；	

续表

控制项	网络安全事件应急预案制定的法规遵从建议	对应条款
应急响应 日常运行 小组	参与和协助应急预案的测试、培训和演练； 维护和管理应急预案文档； 网络安全事件发生时的损失控制和损害评估	
3. 网络安全事件应急响应流程		
网络安全 监测与 预警	<p>预警分级：网络安全事件预警等级分为四级，由高到低依次用红色、橙色、黄色和蓝色表示，分别对应发生或可能发生特别重大、重大、较大和一般网络安全事件。</p> <p>预警监测：组织应按照“谁主管谁负责、谁运行谁负责”的要求，组织对本单位建设运行的网络和信息系统开展网络安全监测工作。</p> <p>预警研判和发布：组织应对监测信息进行研判，认为需要立即采取防范措施的，应当及时通知有关部门和单位，对可能发生重大及以上网络安全事件的信息及时向应急办报告。预警信息包括事件的类别、预警级别、起始时间、可能影响范围、警示事项、应采取的措施和时限要求、发布机关等。</p> <p>预警响应：组织应当按照国家发布的红色、橙色、黄色、蓝色预警进行预警响应。</p> <p>预警解除：组织应当依据有关部门发布的预警解除信息解除预警措施</p>	
应急处置	<p>事件报告：网络安全事件发生后，组织应立即启动应急预案，实施处置并及时报送信息。</p> <p>应急响应：网络安全事件应急响应分为四级，分别对应特别重大、重大、较大和一般网络安全事件。I 级为最高响应级别。组织应当按照不同的级别进行应急响应</p>	
调查与 评估	原则上，组织应在应急响应结束后 30 天内完成事件的调查与评估，针对事件的起因、性质、影响、责任等进行分析评估，提出处理意见和改进措施	

续表

控制项	网络安全事件应急预案制定的法规遵从建议	对应条款
4. 网络安全事件分类应急处置措施		
有害程序事件	针对病毒及破坏性程序蔓延的情况，应由应急响应组织进行处置，可以协调外部组织进行技术协助，分析有害程序，保护现场，必要时切断相关网络连接。应急响应组织先完成有害程序清除方案，并对方案进行验证，保证清除方案对业务无影响。再清除有害程序，恢复受影响网络和信息系统的正常运行	
网络攻击事件	应急响应组织通过入侵检测和安全审计等方法确定攻击方法，采取措施保护现场，阻止攻击行为进一步造成危害。应急响应组织还需对现场进行全面勘查取证，查明网络攻击来源	
信息破坏事件	应急响应组织对被泄露、窃取和丢失的秘密信息进行鉴定，确定信息的密级，确定泄密事件的性质。并对现场进行全面勘查取证，分析判断，查明泄密的渠道，确定窃密对象。应急响应组织需要采取有效措施，阻断泄密渠道	
信息内容安全事件	应急响应组织对利用信息网络发布危害国家安全、社会稳定和公共利益的内容，需要对内容进行删除或屏蔽，并对发布内容的人员权限进行管制。对重大事件需要进行紧急外部通告，消除或降低事件影响	
设备设施故障	应急响应组织及时修复设备故障，不能修复的设备，信息系统建设管理责任部门要立即进行更换，保障网络的畅通和重要信息系统的正常运行。应急响应组织及时查明设备设施故障的原因，完善设备部分方案	

续表

控制项	网络安全事件应急预案制定的法规遵从建议	对应条款
灾害性事件	应急响应组织对事件进行内部和外部进行紧急通报，并协调外部组织协助应急响应组织对网络和信息系统的受损情况进行调查，并对灾害性事件进行评估，充分评估涉及部门、业务范围和社会影响。评估后，对发生事件的网络和信息系系统应尽快恢复信息系统的正常运行。	
其他安全事件	应急响应组织对各种其他安全事件，特别是与自身业务、自身系统、设备特殊性相关的安全事件的处理，需要有应急处置专门措施，如工业网络安全领域的安全事件，需要有专门的应急处置措施	

三、监督管理与法律责任

《网络安全法》第八条规定，国家网信部门负责统筹协调网络安全工作和相关监督管理工作。国务院电信主管部门、公安部门和其他有关机关依照本法和有关法律、行政法规的规定，在各自职责范围内负责网络安全保护和监督管理工作。县级以上地方人民政府有关部门的网络安全保护和监督管理职责，按照国家有关规定确定。由此可见，国家网信部门负责统筹协调网络安全事件应急预案的制定和实施，国务院电信主管部门、公安部门和其他有关机关依照《网络安全法》和有关法律、行政法规的规定，在各自职责范围内负责网络安全事件应急预案制定和实施的监督管理工作。

在法律责任方面，针对网络运营者不履行《网络安全法》第二十五条规定的网络安全保护义务，没有制定网络安全事件应急预案的，由网络运营者的有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处一万元以上十万元以下罚款，对直接负责的主管人员处五千元以上五万元以下罚款。此外，针对关键信息基础设施的运营者不履行《网络安全法》第三十四条第四款规定的网络安全保护义务，没有制定网络安全事件应急预案的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。



## 第六节 网络安全事件应急响应机制

网络安全事件发生后，及时启动应急预案是确保损失最小化的重要举措，而协调有力的应急响应组织机构和完善的应急响应程序是应急预案有效执行的保障。网络安全事件的应急响应涉及多个部门，既要明确统筹协调机构的职责，也要明确其他机构的配合机制。发生网络安全事件，为确保及时报告和实现应急响应，必须明确操作标准和责任主体，避免相互推诿、贻误时机。应急响应是特殊状态，符合条件时也应及时按照程序结束应急响应。严格按照程序执行网络安全事件应急响应机制，是实现应急响应有力、有序、有效的保障。

### 一、《网络安全法》相关规定及释义

#### （一）网络安全事件应急响应的组织机构及其工作机制

《网络安全法》第五十三条规定，国家网信部门协调有关部门建立健全网络安全风险评估和应急工作机制，制定网络安全事件应急预案，并定期组织演练。由此可见，国家网信部门负责协调有关部门建立其内部的网络安全事件应急响应的组织机构体系，并完善其相应的应急响应工作机制。因此，有关部门应当按照要求建立健全其组织内部的网络安全事件应急响应体制机制。

具体而言，根据《国家网络安全事件应急预案》规定，在中央网络安全和信息化领导小组的领导下，中央网络安全和信息化领导小组办公室统筹协调组织国家网络安全事件的应急响应工作，建立健全跨部门联动处置机制，工业和信息化部、公安部、国家保密局等相关部门按照职责分工负责相关网络安全事件应对工作。必要时成立国家网络安全事件应急指挥部（以下简称“指挥部”），负责特别重大网络安全事件处置的组织指挥和协调。国家网络安全应急办公室（以下简称“应急办”）设在中央网信办，具体工作由中央网信办网络安全协调局承担。

中央和国家机关各部门按照职责和权限，负责本部门、本行业网络和信息系  
统网络安全事件的应急处置工作。各省（区、市）网信部门在本地区党委网络安  
全和信息化领导小组统一领导下，统筹协调组织本地区网络和信息系网络安全  
事件的应急处置工作。

## （二）网络安全事件报告

《网络安全法》第五十五条规定，发生网络安全事件，应当立即启动网络安全  
事件应急预案，对网络安全事件进行调查和评估，要求网络运营者采取技术措施  
和其他必要措施，消除安全隐患，防止危害扩大，并及时向社会发布与公众有关  
的警示信息。具体而言，根据《国家网络安全事件应急预案》规定，网络安全事  
件发生后，事发单位应立即启动应急预案，实施处置并及时报送信息。有关地  
区、部门立即组织先期处置，控制事态，消除隐患，同时组织研判，注意保存证  
据，做好信息通报工作。对于初判为特别重大、重大网络安全事件的，立即报告  
应急办。

## （三）网络安全事件应急响应措施

网络安全事件应急响应分为 I 级响应、II 级响应、III 级响应、IV 级响应四级，  
分别对应特别重大、重大、较大和一般网络安全事件，其中 I 级为最高响应级别。  
网络安全事件应急响应机制的建立及其具体应急响应措施应当根据网络安全事件  
的不同等级予以落实。

具体而言，属特别重大网络安全事件的，应当及时启动 I 级响应，成立指挥  
部，履行应急处置工作的统一领导、指挥、协调职责，应急办 24 小时值班。有关  
省（区、市）、部门应急指挥机构进入应急状态，在指挥部的统一领导、指挥、协  
调下，负责本省（区、市）、本部门应急处置工作或支援保障工作，24 小时值班，  
并派员参加应急办工作。有关省（区、市）、部门跟踪事态发展，检查影响范围，  
及时将事态发展变化情况、处置进展情况报应急办。指挥部对应对工作进行决策  
部署，有关省（区、市）和部门负责组织实施。

网络安全事件的 II 级响应，由有关省（区、市）和部门根据事件的性质和

情况确定：①事件发生省（区、市）或部门的应急指挥机构进入应急状态，按照相关应急预案做好应急处置工作；②事件发生省（区、市）或部门及时将事态发展变化情况报应急办，应急办将有关重大事项及时通报相关地区和部门；③处置中需要其他有关省（区、市）、部门和国家网络安全应急技术支撑队伍配合和支持的，报告应急办予以协调，相关省（区、市）、部门和国家网络安全应急技术支撑队伍应根据各自职责，积极配合、提供支持；④有关省（区、市）和部门根据应急办的通报，结合各自实际有针对性地加强防范，防止造成更大范围影响和损失。

III级、IV级响应，由事件发生地区和部门按相关预案进行应急响应。

#### （四）网络安全事件应急响应结束及其事后调查评估

《国家网络安全事件应急预案》规定，结束 I 级响应的，由应急办提出建议，报指挥部批准后，及时通报有关省（区、市）和部门。结束 II 级响应的，由事件发生省（区、市）或部门决定，报应急办，应急办通报相关省（区、市）和部门。

特别重大网络安全事件由应急办组织有关部门和省（区、市）进行调查处理和总结评估，并按程序上报。重大及以下网络安全事件由事件发生地区或部门自行组织调查处理和总结评估，其中重大网络安全事件相关总结调查报告报应急办。总结调查报告应对事件的起因、性质、影响、责任等进行分析评估，提出处理意见和改进措施。事件的调查处理和总结评估工作原则上在应急响应结束后 30 天内完成。

## 二、网络安全事件应急响应的法规遵从框架及建议

网络安全事件应急响应机制包括网络安全事件应急响应技术措施、组织机构和保障措施等方面，网络运营者应当重点关注《网络安全法》、《关键信息基础设施安全保护条例（征求意见稿）》、《国家网络安全事件应急预案》及行业网络安全事件应急管理的规范性文件等，建立和完善其内部的网络安全事件应急响应机制。

网络安全事件应急响应的法规遵从框架如表 7-11 所示。

表 7-11 网络安全事件应急响应的法规遵从框架

法律名称	法律条款	法律规定
《网络安全法》	第二十五条	网络运营者应当制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险；在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告
	第五十三条	国家网信部门协调有关部门建立健全网络安全风险评估和应急工作机制，制定网络安全事件应急预案，并定期组织演练
	第五十五条	发生网络安全事件，应当立即启动网络安全事件应急预案，对网络安全事件进行调查和评估，要求网络运营者采取技术措施和其他必要措施，消除安全隐患，防止危害扩大，并及时向社会发布与公众有关的警示信息
《关键信息基础设施安全保护条例（征求意见稿）》	第三十九条	<p>国家网信部门按照国家网络安全事件应急预案的要求，统筹有关部门建立健全关键信息基础设施网络安全应急协作机制，加强网络安全应急力量建设，指导协调有关部门组织跨行业、跨地域网络安全应急演练。</p> <p>国家行业主管或监管部门应当组织制定本行业、本领域的网络安全事件应急预案，并定期组织演练，提升网络安全事件应对和灾难恢复能力。发生重大网络安全事件或接到网信部门的预警信息后，应立即启动应急预案组织应对，并及时报告有关情况</p>
《国家网络安全事件应急预案》	4.2 应急响应	<p>网络安全事件应急响应分为四级，分别对应特别重大、重大、较大和一般网络安全事件。I 级为最高响应级别。</p> <p><b>4.2.1 I 级响应</b></p> <p>属特别重大网络安全事件的，及时启动 I 级响应，成立指挥部，履行应急处置工作的统一领导、指挥、协调职责。应急办 24 小时值班。</p> <p>有关省（区、市）、部门应急指挥机构进入应急状态，在指挥部的统一领导、指挥、协调下，负责本省（区、市）、本部门应急处置工作或支援保障工作，24 小时值班，并派员参加应急办工作。</p> <p>有关省（区、市）、部门跟踪事态发展，检查影响范围，及时将事态发展变化情况、处置进展情况报应急办。指挥部对应对工作进行决策部署，有关省（区、市）和部门负责组织实施。</p> <p><b>4.2.2 II 级响应</b></p> <p>网络安全事件的 II 级响应，由有关省（区、市）和部门根据事件的性质和情况确定。</p> <p>（1）事件发生省（区、市）或部门的应急指挥机构进入应急状态，按照相关应急预案做好应急处置工作。</p> <p>（2）事件发生省（区、市）或部门及时将事态发展变化情况报应急办。应急办将有关重大事项及时通报相关地区和部门。</p>

续表

法律名称	法律条款	法律规定
《国家网络安全事件应急预案》	4.2 应急响应	<p>(3) 处置中需要其他有关省（区、市）、部门和国家网络安全应急技术支撑队伍配合和支持的，报告应急办予以协调。相关省（区、市）、部门和国家网络安全应急技术支撑队伍应根据各自职责，积极配合、提供支持。</p> <p>(4) 有关省（区、市）和部门根据应急办的通报，结合各自实际有针对性地加强防范，防止造成更大范围影响和损失。</p> <p>4.2.3 III级、IV级响应</p> <p>事件发生地区和部门按相关预案进行应急响应</p>
	4.3 应急结束	<p>4.3.1 I 级响应结束</p> <p>应急办提出建议，报指挥部批准后，及时通报有关省（区、市）和部门。</p> <p>4.3.2 II 级响应结束</p> <p>由事件发生省（区、市）或部门决定，报应急办，应急办通报相关省（区、市）和部门</p>
	7 保障措施	<p>7.1 机构和人员</p> <p>各地区、各部门、各单位要落实网络安全应急工作责任制，把责任落实到具体部门、具体岗位和个人，并建立健全应急工作机制。</p> <p>7.2 技术支撑队伍</p> <p>加强网络安全应急技术支撑队伍建设，做好网络安全事件的监测预警、预防防护、应急处置、应急技术支援工作。支持网络安全企业提升应急处置能力，提供应急技术支援。中央网信办制定评估认定标准，组织评估和认定国家网络安全应急技术支撑队伍。各省（区、市）、各部门应配备必要的网络安全专业技术人才，并加强与国家网络安全相关技术单位的沟通、协调，建立必要的网络安全信息共享机制。</p> <p>7.3 专家队伍</p> <p>建立国家网络安全应急专家组，为网络安全事件的预防和处置提供技术咨询和决策建议。各地区、各部门加强各自的专家队伍建设，充分发挥专家在应急处置工作中的作用。</p> <p>7.4 社会资源</p> <p>从教育科研机构、企事业单位、协会中选拔网络安全人才，汇集技术与数据资源，建立网络安全事件应急服务体系，提高应对特别重大、重大网络安全事件的能力。</p> <p>7.5 基础平台</p> <p>各地区、各部门加强网络安全应急基础平台和管理平台建设，做到早发现、早预警、早响应，提高应急处置能力。</p>

续表

法律名称	法律条款	法律规定
《国家网络安全事件应急预案》	7 保障措施	<p><b>7.6 技术研发和产业促进</b></p> <p>有关部门加强网络安全防范技术研究,不断改进技术装备,为应急响应工作提供技术支撑。加强政策引导,重点支持网络安全监测预警、预防防护、处置救援、应急服务等方向,提升网络安全应急产业整体水平与核心竞争力,增强防范和处置网络安全事件的产业支撑能力。</p> <p><b>7.7 国际合作</b></p> <p>有关部门建立国际合作渠道,签订合作协定,必要时通过国际合作共同应对突发网络安全事件。</p> <p><b>7.8 物资保障</b></p> <p>加强对网络安全应急装备、工具的储备,及时调整、升级软件硬件工具,不断增强应急技术支撑能力。</p> <p><b>7.9 经费保障</b></p> <p>财政部门为网络安全事件应急处置提供必要的资金保障。有关部门利用现有政策和资金渠道,支持网络安全应急技术支撑队伍建设、专家队伍建设、基础平台建设、技术研发、预案演练、物资保障等工作开展。各地区、各部门为网络安全应急工作提供必要的经费保障。</p> <p><b>7.10 责任与奖惩</b></p> <p>网络安全事件应急处置工作实行责任追究制。</p> <p>中央网信办及有关地区和部门对网络安全事件应急管理工作中做出贡献的先进集体和个人给予表彰和奖励。</p> <p>中央网信办及有关地区和部门对不按照规定制定预案和组织开展演练,迟报、谎报、瞒报和漏报网络安全事件重要情况或者应急管理工作中有其他失职、渎职行为的,依照相关规定对有关责任人给予处分;构成犯罪的,依法追究刑事责任</p>
《银行业重要信息系统突发事件应急管理规范(试行)》	第三十二条	银行业金融机构应按照本机构既定的应急预案,做好应急处置,快速有效处置突发事件
	第三十三条	<p>银行业金融机构风险管理部门应在董事会和高管层授权下负责突发事件报告,并指定专人为报告责任人。当报告责任人确定或发生变更时应及时向银监会或其派出机构信息系统应急管理部门报备。</p> <p>当多个重要信息系统同时受到影响时,按照受影响程序最高原则报告</p>
	第三十四条	<p>全国性银行业金融机构总部向银监会信息系统应急管理部门报告;</p> <p>全国性银行业金融机构的一级分支机构、地方性银行业金融机构向当地银监会派出机构信息系统应急管理部门报告</p>

续表

法律名称	法律条款	法律规定
《银行业重要信息系统突发事件应急管理规范（试行）》	第三十五条	<p>突发事件应急响应流程：</p> <p>（一）应急执行小组应根据既定的应急预案，启动应急操作，并及时报告应急领导小组。应急处置应集中于建立临时业务处理能力、修复原系统损害、在原系统或新设施中恢复运行业务能力等应急措施；</p> <p>（二）对于应急预案没有覆盖的突发事件，应立即报告应急领导小组进行应急决策；</p> <p>（三）应急领导小组应立即启动本机构应急组织，组织协调机构内部进行应急处置，并负责向监管部门报告应急响应情况；</p> <p>（四）支持保障小组做好各项应急保障工作，为应急处置提供场地、交通、通信及其他后勤保障；</p> <p>（五）银行业金融机构应在重要信息系统突发事件后 60 分钟之内将突发事件相关情况上报银监会或其派出机构信息系统应急管理部门，并在事件发生后 12 小时内提交正式书面报告；</p> <p>（六）对造成经济秩序混乱或重大经济损失、影响金融稳定的，或者对银行、客户、公众的利益造成损害的突发事件，银行业金融机构要立即上报；</p> <p>（七）银行业金融机构应将应急处置重大进展情况及时上报银监会或其派出机构，直至应急结束。Ⅰ级突发事件发生后，银行业金融机构应每 2 小时将应急处置进展情况上报，直至应急结束</p>
	第三十六条	上报银监会或其派出机构的局面报告内容应包括突发事件时间、地点、现象、影响的业务范围、原因分析、后果的初步判断、已采取的措施，后续拟采取方案的建议、事件报告单位、联系人及联系方式、其他与本突发事件有关的内容，并在报告中重点明确需要银监会协调的事项
	第三十七条	银监会及其派出机构信息系统应急管理部门根据银行业金融机构应急协调需求，组织协调国家信息化管理、信息安全管理、治安管理等跨部门资源，统筹安排处置工作
	第三十八条	应急处置中所有相关的信息和处理过程应进行严格记录，外部供应商的处理过程应有专门记录文件，如果涉及保险理赔，中间过程和场景可用摄像设备进行记录。所有过程资料应由专人存档保管
《工业控制系统信息安全事件应急管理工作指南》	第二十一条	工业和信息化部、地方工业和信息化主管部门、工业企业制定本级工控安全事件应急预案，定期组织应急演练
《工业控制系统信息安全防护指南》	第七条	制定工控安全事件应急响应预案，当遭受安全威胁导致工业控制系统出现异常或故障时，应立即采取紧急防护措施，防止事态扩大，并逐级报送直至属地省级工业和信息化主管部门，同时注意保护现场，以便进行调查取证

续表

法律名称	法律条款	法律规定
《证券期货业信息安全保障管理办法》	第四十七条	中国证监会组织制定证券期货业信息安全应急预案，督促、指导行业开展信息安全应急工作
《公共互联网网络安全威胁监测与处置办法》	第十三条	造成或可能造成严重社会危害或影响的公共互联网网络安全突发事件的监测与处置工作，按照国家和电信主管部门有关应急预案执行

网络安全事件应急响应涵盖应急启动、应急处置、事后恢复等网络安全事件管理的全生命周期。因此，针对网络安全事件应急响应的法规遵从要求，网络运营者应当重点关注表 7-12 中的几个方面。

表 7-12 网络安全事件应急响应的法规遵从建议

控制项	网络安全事件应急响应的法规遵从建议	对应条款
1. 事件通告		第二十五条 网络运营者应当制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险；在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告。
信息通报	<p>组织内信息通报</p> <p>在网络安全事件发生后，应通知应急响应日常运行小组使其能够确定事态的严重程度和下一步将要采取的行动。在损害评估完成后，应通知应急响应领导小组。可以通过各种方法完成通知，包括固定电话、移动电话和电子邮件等。由于电子邮件无法确定能否有效回复，所以通过电子邮件发送通知应谨慎从事。</p> <p>组织外信息通报</p> <p>网络安全事件发生后，应将相关信息及时通报给受到负面影响的外部机构、互联的单位系统以及重要客户，同时根据应急响应的需要，应将相关信息准确通报给相关设备及服务提供商、电信、电力等外部组织，以获得适当的应急响应支持。对外信息通报应符合组织的对外信息发布策略</p>	第五十三条 国家网信部门协调有关部门建立健全网络安全风险评估和应急工作机制，制定网络安全事件应急预案，并定期组织演练。
信息上报	网络安全事件发生后，应按照相关规定和要求，及时将情况上报相关单位或部门	负责关键信息基础设施安全保护工作的部门应当制定本行业、本领域的网络安全事件应急预案，并定期组织演练。
信息披露	网络安全事件发生后，根据网络安全事件的严重程度，组织应指定特定的小组及时向新闻媒体发布相关信息，指定的小组应严格按照组织相关规定和要求对外发布信息，同时组织内其他部门或者个人不得随意接受新闻媒体采访或对外发表自己的看法	
2. 事件分类与定级		
	组织应当依据《国家网络安全事件应急预案》确定的网络安全事件分类分级标准对发生的网络安全事件进行分类与分级	



续表

控制项	网络安全事件应急响应的法规遵从建议	对应条款
3. 应急启动		<p>网络安全事件应急预案应当按照事件发生后的危害程度、影响范围等因素对网络安全事件进行分级，并规定相应的应急处置措施。</p> <p>第五十五条 发生网络安全事件，应当立即启动网络安全事件应急预案，对网络安全事件进行调查和评估，要求网络运营者采取技术措施和其他必要措施，消除安全隐患，防止危害扩大，并及时向社会发布与公众有关的警示信息</p>
启动原则	组织应确保其针对网络安全事件的应急启动具体操作遵循快速和有序的规则	
启动依据	网络安全事件应急响应分为四级，分别对应特别重大、重大、较大和一般网络安全事件。I 级为最高响应级别。一般而言，对于导致业务中断、系统宕机、网络瘫痪等突发/重大网络安全事件应立即启动应急。但由于组织规模、构成、性质等的不同，不同组织对突发/重大网络安全事件的定义可能不一样，因此，各组织的应急启动条件可能各不相同。启动条件可以基于以下方面考虑：人员的安全和/或设施损失的程度；系统损失的程度（如物理的、运作的或成本的）；系统对于组织使命的影响程度（如保护资产的关键基础设施）；预期的中断持续时间等。只有当损害评估的结果显示一个或多个系统启动条件被满足时，应急预案才应被启动	
启动方法	由应急响应领导小组发布应急响应启动令。应急响应启动后应急响应领导小组要对人力、财力、物力到位情况实施检查与督察，并记录实际发生情况	
4. 应急处置		
恢复顺序	当恢复复杂系统时，恢复进程应反映出组织确定的系统优先顺序。恢复的顺序应反映出系统允许的中断时间，以避免对相关系统及业务的重大影响	
恢复规程	获得访问受损设施或地理区域的授权； 通知相关系统的内部和外部业务伙伴； 获得所需的办公用品和工作空间； 获得安装所需的硬件部件； 获得装载备份介质； 恢复关键操作系统和应用软件； 恢复系统数据； 成功运行备用设备	
网络安全事件分类应急处置措施	有害程序事件  病毒及破坏性程序蔓延的，由应急响应组织进行处置，可以协调外部组织进行技术协助，分析有害程序，保护现场，必要时切断相关网络连接。应急响应组织先完成有害程序清除方案，并对方案进行验证，保证清除方案对业务无影响。再清除有害程序，恢复受影响网络和信息系统的正常运行	

续表

控制项	网络安全事件应急响应的法规遵从建议	对应条款	
网络安全事件分类应急处置措施	网络攻击事件 应急响应组织通过入侵检测和安全审计等方法确定攻击方法，采取措施保护现场，阻止攻击行为进一步造成危害。应急响应组织还需对现场进行全面勘查取证，查明网络攻击来源。		
	信息破坏事件 应急响应组织对被泄露、窃取和丢失的秘密信息进行鉴定，确定信息的密级，确定泄密事件的性质。对现场进行全面勘查取证，分析判断，查明泄密的渠道，确定窃密对象。应急响应组织需要采取有效措施，阻断泄密渠道。		
	信息内容安全事件 应急响应组织对利用信息网络发布危害国家安全、社会稳定和公共利益的内容，需要对内容进行删除或屏蔽，并对发布内容的人员权限进行管制。对重大事件需要进行紧急外部通告，消除或降低事件影响。		
	设备设施故障 应急响应组织及时修复设备故障，不能修复的设备，信息系统建设管理责任部门要立即进行更换，保障网络的畅通和重要信息系统的正常运行。应急响应组织及时查明设备设施故障的原因，完善设备部分方案。		
	灾害性事件 应急响应组织对事件进行内部和外部进行紧急通报，并协调外部组织协助应急响应组织对网络和信息系统的受损情况进行调查，并对灾害性事件进行评估，充分评估涉及部门、业务范围和社会影响。评估后，对发生事件的网络和信息系统应尽快恢复信息系统的正常运行。		
	其他安全事件 应急响应组织对各种其他安全事件，特别是跟自身业务、自身系统、设备特殊性相关的安全事件的处理，需要有应急处置专门的措施，比如工业信息安全领域的安全事件，需要有专门的应急处置措施		
	5. 后期处置		
	信息系统重建		在应急处置工作结束后，组织应迅速采取措施，抓紧组织抢修受损的基础设施，减少损失，尽快恢复正常工作。通过统计各种数据，查明原因，对网络安全事件造成的损失和影响，以及恢复重建能力进行分析评估，认真制订恢复重建计划，迅速组织实施信息系统重建

续表

控制项	网络安全事件应急响应的法规遵从建议	对应条款
应急响应总结	应急响应总结是应急处置之后应进行的工作，具体工作包括： 分析和总结事件发生原因； 分析和总结事件现象； 评估系统的损害程度； 评估事件导致的损失； 分析和总结应急处置记录； 评审应急响应措施的效果和效率，并提出改进建议； 评审应急预案的效果和效率，并提出改进建议	
6. 应急响应保障措施		
管理人力保障	组织应落实网络安全应急工作责任制，把责任落实到具体部门、具体岗位和个人，并建立健全应急响应工作机制。 组织应依据自身的职责制定具体角色和职责分工细则，细则需要制度化，并依据现有人员的实际情况制定合理工作安排，工作安排要直接落实到人，形成所有工作人员的独立工作手册，如有人员工作安排变动时要及时更正工作手册。管理人力力的具体保障由应急响应领导小组统一规划和组织管理	
技术人力保障	组织应通过建立应急响应技术保障小组和应急响应专家小组来进行技术人力保障，所有技术保障问题统一由技术保障小组负责，技术保障小组要依据应急的技术需要制定具体角色和职责分工细则，细则需要制度化，并依据现有人员的实际情况制定合理工作安排，工作安排要直接落实到人，形成所有工作人员的独立工作手册，如有人员工作安排变动时要及时更正工作手册。 由于技术保障小组除了建立自身的技术支持队伍外，所确定的角色与职责大多需要依赖合作者（包括社会力量和专家等），所以，技术保障小组要建立完备的技术培训机构和操作管理方案，保证新技术与应急响应技术的及时培训，保证应急响应技术的有效性。 技术保障小组可以依据自身的工作特点、协作单位与人员的具体情况制定应急响应协同调度方案，但无论采取何种方案均要有具体的协同工作记录以备审计	
基础物质保障	组织应保证日常技术保障的实现、日常管理工作的开展和应急响应技术服务在应急响应时的及时到位。物质需求由应急响应技术保障小组提出，应急响应日常运行小组落实	
应急响应物质保障	应急响应物质保障包括财力保障、交通运输保障、治安维护和通信保障等部分。 财力保障：保证所需应急响应资金。	

		续表
控制项	网络安全事件应急响应的法规遵从建议	对应条款
应急响应 物质保障	<p>交通运输保障：协调保证紧急情况下应急交通工具的优先安排、优先调度、优先放行，确保运输安全畅通。</p> <p>通信保障：建立健全应急通信、应急广播电视保障工作体系，完善公用通信网，建立有线和无线相结合、基础电信网络与移动通信系统相配套的应急通信系统，确保通信畅通</p>	
应急响应 技术服务保障	<p>技术保障由应急响应技术保障小组统一负责，依据应急响应的需要，应急响应技术保障小组应制定网络安全事件技术应对表，全面考察和管理相关技术基础，选择合适的技术服务者，明确职责和沟通方式</p>	
日常技术保障	<p>日常技术保障包括事件监控与预警的技术保障，应急技术储备两部分。</p> <p>事件监控与预警的技术保障</p> <p>事件监控与预警的技术保障由应急响应日常运行小组负责。应急响应日常运行小组应保证网络安全事件的快速发现和及时预警。对网络安全事件进行日常监控的方法（手段）、流程、记录等应明确职责，落实到人。</p> <p>应急技术储备</p> <p>应急技术储备由应急响应技术保障小组配合应急处理技术服务和技术人力保障实现</p>	

### 三、监督管理与法律责任

《网络安全法》第八条规定，国家网信部门负责统筹协调网络安全工作和相关监督管理工作。国务院电信主管部门、公安部门和其他有关机关依照本法和有关法律、行政法规的规定，在各自职责范围内负责网络安全保护和监督管理工作。县级以上地方人民政府有关部门的网络安全保护和监督管理职责，按照国家有关规定确定。针对网络安全事件应急响应而言，《国家网络安全事件应急预案》规定，在中央网络安全和信息化领导小组（以下简称“领导小组”）的领导下，中央网络安全和信息化领导小组办公室（以下简称“中央网信办”）统筹协调组织国家网络安全事件应对工作，建立健全跨部门联动处置机制，工业和信息化部、公安部、国家保密局等相关部门按照职责分工负责相关网络安全事件应对工作。必要时成立指挥部，负责特别重大网络安全事件处置的组织指挥和协调。

在网络安全事件应急响应监督管理的具体实施层面，一方面，应急办设在中央网信办，具体工作由中央网信办网络安全协调局承担。应急办负责网络安全应急跨部门、跨地区协调工作和指挥部的事务性工作，组织指导国家网络安全应急技术支撑队伍做好应急处置的技术支撑工作。有关部门派负责相关工作的司局级同志为联络员，联络应急办工作。另一方面，中央和国家机关各部门按照职责和权限，负责本部门、本行业网络和信息系统的网络安全事件的预防、监测、报告和应急处置工作。各省（区、市）网信部门在本地区党委网络安全和信息化领导小组统一领导下，统筹协调组织本地区网络和信息系统的网络安全事件的预防、监测、报告和应急处置工作。

在法律责任方面，《网络安全法》第五十九条规定，网络运营者不履行本法第二十五条规定的网络安全保护义务，没有在发生危害网络安全的事件时立即启动应急预案，采取相应的补救措施，则将由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处一万元以上十万元以下罚款，对直接负责的主管人员处五千元以上五万元以下罚款。此外，关键信息基础设施的运营者不履行《网络安全法》第三十四条规定的网络安全保护义务，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。

## 第七节 网络安全事件应急演练

### 一、《网络安全法》相关规定及释义

《网络安全法》第五十三规定，国家网信部门协调有关部门建立健全网络安全风险评估和应急工作机制，制定网络安全事件应急预案，并定期组织演练。负责关键信息基础设施安全保护工作的部门应当制定本行业、本领域的网络安全事件应急预案，并定期组织演练。此外，《网络安全法》第三十四条第四款规定，关键

信息基础设施的运营者应当制定网络安全事件应急预案，并定期进行演练。

由于网络安全事件应急预案仅仅是对潜在可能发生的网络安全事件的一种预测和应对，为了提升应急预案的科学性、合理性、针对性和可操作性，应急预案编制单位应当建立应急演练制度，根据实际情况采取实战演练等方式，定期组织开展人员广泛参与、处置联动性强、形式多样、节约高效的应急演练。通过实践，发现应急预案中存在的问题与不足，及时进行改进，增强应急预案的合理性和可操作性，提升应急预案编制单位的实际应对能力和操作能力，在一定程度上也可以有效减少网络安全事件发生后造成的损失。

### （一）网络安全事件应急演练的主体

《网络安全法》规定的网络安全事件应急演练涉及的主体包括三方面：一是国家网信部门协调有关部门组织演练，二是负责关键信息基础设施安全保护工作的部门组织本行业、本领域的应急演练，三是关键信息基础设施的运营者定期进行应急演练。由此可以看出，国家网信部门是网络安全事件应急演练的协调者，关键信息基础设施安全保护工作的部门（通常为关键信息基础设施行业主管或监管部门）是本行业、本领域的网络安全事件应急演练的组织者，关键信息基础设施的运营者是应急演练的具体实施者。

除此以外，网络安全事件应急演练也比较常见。例如，工信部组织通信行业开展互联网安全应急演练、证监会组织证券期货业开展网络安全联合应急演练等。许多组织、企业等还开展本组织、企业的演练。我国有的机构还参加国际网络安全演练。例如，国家计算机网络应急技术处理协调中心多次参加亚太地区、东盟地区网络安全应急演练。

### （二）网络安全事件应急演练的频率

《网络安全法》规定的演练应当定期进行，目的是加强应急演练的常态化、机制化，而不是时断时续、可有可无。《国家网络安全事件应急预案》规定，中央网信办协调有关部门定期组织演练，检验和完善预案，提高实战能力。各省（区、市）、各部门每年至少组织一次预案演练，并将演练情况报中央网信办。中央网信办及有关地区和部门对不按照规定制定预案和组织开展演练的，依照相关规定对

有关责任人给予处分；构成犯罪的，依法追究刑事责任。《突发事件应急预案管理办法》第二十二条中规定：专项应急预案、部门应急预案至少每3年进行一次应急演练。地震、台风、洪涝、滑坡、山洪泥石流等自然灾害易发区域所在地政府，重要基础设施和城市供水、供电、供气、供热等生命线工程经营管理单位，矿山、建筑施工单位和易燃易爆物品、危险化学品、放射性物品等危险物品生产、经营、储运、使用单位，公共交通工具、公共场所和医院、学校等人员密集场所的经营单位或者管理单位等，应当有针对性地经常组织开展应急演练。《生产安全事故应急预案管理办法》第三十三条规定：生产经营单位应当制定本单位的应急预案演练计划，根据本单位的事故风险特点，每年至少组织一次综合应急预案演练或者专项应急预案演练，每半年至少组织一次现场处置方案演练。《国家核应急预案》规定：国家级核事故应急联合演习由国家核应急协调委组织实施，一般3~5年举行一次；国家核应急协调委成员单位根据需要分别组织单项演练。省级核应急联合演习，一般2~4年举行一次，由省核应急委组织，核设施营运单位参加。核设施营运单位综合演习每2年组织1次，拥有3台以上运行机组的，综合演习频度适当增加。

除了法律规定必须进行的应急演练以外，实践中有关方面通常还会自行安排演练。值得注意的是，如果演练过于频繁，会增加企业、关键信息基础运营者等相关主体的负担，也容易导致参与演练各方为了应付演练而走形式，达不到演练的预期效果，所以必须科学安排应急演练的频率。

### （三）网络安全事件应急演练方案的制定和效果评估

演练可以是综合性的，也可以是专项演练，需要根据网络安全形势发展的实际情况而定，需要特别注意网络安全威胁场景的变化和更新，制定有针对性的演练方案。

《突发事件应急预案管理办法》第二十三条规定：应急演练组织单位应当组织演练评估。评估的主要内容包括：演练的执行情况，预案的合理性与可操作性，指挥协调和应急联动情况，应急人员的处置情况，演练所用设备装备的适用性，对完善预案、应急准备、应急机制、应急措施等方面的意见和建议等。鼓励委托第三方进行演练评估。《生产安全事故应急预案管理办法》第三十四条规定：应急

预案演练结束后，应急预案演练组织单位应当对应急预案演练效果进行评估，撰写应急预案演练评估报告，分析存在的问题，并对应急预案提出修订意见。上述规定对网络安全事件应急预案演练的具体实施具有借鉴意义。

二、典型案例<sup>①</sup>

2017 年 3 月，江苏南通移动组织开展专项应急演练，以提升应急处置能力，为网络与网络安全保障护航。演练现场，南通移动技术人员模拟自有网站被篡改、WLAN 网络有漏洞等实战情境，紧急开展应急处置，在 5 分钟内及时发现并恢复正常页面，并对 WLAN 网络进行了安全加固。此外，南通移动还对自有服务器设备进行了全量高危漏洞扫描，确保不存在安全隐患。

三、网络安全事件应急演练的法规遵从框架及建议

网络运营者应当重点关注《网络安全法》、《关键信息基础设施安全保护条例（征求意见稿）》、《国家网络安全事件应急预案》以及行业网络安全事件应急演练的规范性文件等，针对网络安全事件应急演练的法规遵从框架（见表 7-13）进行整体把握。

表 7-13 网络安全事件应急演练的法规遵从框架

法律名称	法律条款	法律规定
《网络安全法》	第三十四条	除本法第二十一条的规定外，关键信息基础设施的运营者还应当履行下列安全保护义务： （四）制定网络安全事件应急预案，并定期进行演练
	第五十三条	国家网信部门协调有关部门建立健全网络安全风险评估和应急工作机制，制定网络安全事件应急预案，并定期组织演练。 负责关键信息基础设施安全保护工作的部门应当制定本行业、本领域的网络安全事件应急预案，并定期组织演练
《关键信息基础设施安全保护条例（征求意见稿）》	第二十五条	运营者网络安全管理负责人履行下列职责： （四）组织开展网络安全检查和应急演练，应对处置网络安全事件

<sup>①</sup> 参考 [http://www.cnii.com.cn/city/2017-03/31/content\\_1839013.htm](http://www.cnii.com.cn/city/2017-03/31/content_1839013.htm)。



续表

法律名称	法律条款	法律规定
《关键信息基础设施安全保护条例（征求意见稿）》	第三十九条	<p>国家网信部门按照国家网络安全事件应急预案的要求，统筹有关部门建立健全关键信息基础设施网络安全应急协作机制，加强网络安全应急力量建设，指导协调有关部门组织跨行业、跨地域网络安全应急演练。</p> <p>国家行业主管或监管部门应当组织制定本行业、本领域的网络安全事件应急预案，并定期组织演练，提升网络安全事件应对和灾难恢复能力。发生重大网络安全事件或接到网信部门的预警信息后，应立即启动应急预案组织应对，并及时报告有关情况</p>
	6.2 演练	<p>中央网信办协调有关部门定期组织演练，检验和完善预案，提高实战能力。</p> <p>各省（区、市）、各部门每年至少组织一次预案演练，并将演练情况报中央网信办</p>
《国家网络安全事件应急预案》	7.10 责任与奖惩	<p>中央网信办及有关地区和部门对不按照规定制定预案和组织开展演练，迟报、谎报、瞒报和漏报网络安全事件重要情况或者应急管理工作中有其他失职、渎职行为的，依照相关规定对有关责任人给予处分；构成犯罪的，依法追究刑事责任</p>
《银行业重要信息系统突发事件应急管理规范（试行）》	第二十二 条	<p>银行业金融机构应定期对应急预案进行测试和演练，确保其有效性</p>
	第二十三 条	<p>当信息系统发生系统上线、系统升级、网络改造、设备更新、配置参数调整等变更时应及时更新应急预案，并适时实施演练</p>
	第二十四 条	<p>银行业金融机构应制订年度信息系统应急演练计划，明确演练的时间、内容、依据、目的、负责人和相关配合机构等要素。演练计划应涵盖对应急预案各环节的检验，验证应急预案的有效性、应急资源的完备性及应急人员的适应性。应急演练应做到全面演练和专项演练相结合，一般情况下，银行业金融机构每年至少应组织一次全系统范围内的应急演练</p>
	第二十五 条	<p>银行业金融机构应严格按照应急演练计划实施应急演练，并注意如下事项：</p> <p>（一）以应急预案为基础，制定应急演练总体方案，并进行风险再评估，制定相应的保障措施；</p> <p>（二）应急演练内容应全面完整，涵盖信息系统的各类应急场景；</p> <p>（三）严格控制应急演练引起的信息系统变更风险，避免因演练导致服务中断；</p>

续表

法律名称	法律条款	法律规定
《银行业重要信息系统突发事件应急管理规范（试行）》	第二十五条	（四）应急演练应选择在非主要业务时段进行； （五）应急演练完成后，应保证实施应急预案所需的各项资源恢复正常； （六）定期对信息系统应急响应相关人员进行培训
	第二十六条	银行业金融机构应积极配合其他业务相关机构完成跨机构或跨行业应急演练
	第二十七条	银行业金融机构在应急演练的过程中，对可能存在较大风险的演练（如全系统范围的演练），应按属地监管原则，在实施演练前将应急演练计划向银监会或其派出机构报备
	第二十八条	应急演练结束后，银行业金融机构应撰写应急演练情况总结报告，大型或重要的应急演练总结报告应提交董事会和高管层。总结报告包括但不限于：内容和目的、总体方案、参与人员、准备工作、主要过程和关键时间点记录、存在的问题、后续改进措施及实施计划、演练结论
	第二十九条	银行业金融机构应根据演练总结报告提出的改进措施进行整改，及时修订相应的应急预案，并组织审计部门对整改情况进行监督和检查
	第三十条	对于全系统范围的年度演练或跨机构和跨行业的演练，银行业金融机构应将演练总结报告上报银监会或其派出机构
	第三十一条	银行业金融机构在应急演练过程中，应根据审计、监管部门要求，将应急演练计划、过程记录和结果分析等归档
《工业控制系统信息安全事件应急管理工作指南》	第二十一条	工业和信息化部、地方工业和信息化主管部门、工业企业制定本级工控安全事件应急预案，定期组织应急演练
《工业控制系统信息安全防护指南》	第七条	定期对工业控制系统的应急响应预案进行演练，必要时对应急响应预案进行修订
《公共互联网网络安全威胁监测与处置办法》	第十三条	造成或可能造成严重社会危害或影响的公共互联网网络安全突发事件的监测与处置工作，按照国家和电信主管部门有关应急预案执行
《电信网络运行监督管理办法》	第四十四条	基础电信业务经营者有下列行为之一，电信监管部门应当予以警告并责令其限期改正。逾期未改正的，可以在行业内予以通报批评。 （三）未制定和演练网络运行事故应急处置预案的

针对网络安全事件应急演练的法规遵从建议（见表 7-14），网络运营者应全面关注其在网络安全事件应急演练计划阶段、准备阶段、实施阶段以及改进阶段应当采取的措施和满足的具体要求。

表 7-14 网络安全事件应急演练的法规遵从建议

控制项	网络安全事件应急演练的遵从要求	对应条款
1. 网络安全事件应急演练计划阶段		第三十四条 除本法第二十一条的规定外，关键信息基础设施的运营者还应当履行下列安全保护义务：  （四）制定网络安全事件应急预案，并定期进行演练。  第五十三条 国家网信部门协调有关部门建立健全网络安全风险评估和应急工作机制，制定网络安全事件应急预案，并定期组织演练。  负责关键信息基础设施安全保护工作的部门应当制定本行业、本领域的网络安全事件应急预案，并定期组织演练
应急演练需求梳理	组织应按照政府、监管单位或上级要求及本单位自主决策进行网络安全事件应急演练，并制订网络安全事件应急演练计划，包括演练的大体内容、形式与频次等。  组织应调研应急演练的具体需求。通过梳理本单位的应急响应预案和应急演练要求等，确定应急演练的主要内容；同时通过风险评估的方式，修订应急演练的内容。  组织应按照各自的应急演练基础条件和保障条件，确定适合各自单位自身的演练目的和演练形式	
2. 网络安全事件应急演练准备阶段		
应急演练组织机构	组织应建立应急演练领导小组、应急演练管理小组、应急演练技术小组、应急演练评估小组、应急响应实施组等应急演练组织机构	
应急演练工作方案	组织应先制定演练工作方案，依次确定以下内容。 应急演练目的：具体的针对性，或者日常常规应急演练； 应急演练等级：依据演练目的制定； 应急演练范围：确定参加演练单位及人员； 应急演练科目、子目、安全事件诱因样例：依据所辖网络的具体安全需求，选择适当的安全事件诱因样例； 应急演练形式，构建应急演练平台，设置网络安全事件现场； 应急演练启动时间； 应急演练效果评价标准：判断演练效果及价值。 应急演练工作方案内容包括：指导思想、工作原则、演练目的、演练场景、演练时间地点、组织体系及职责、演练流程、其他准备事项、工作要求及有关附件等	
应急演练脚本	组织应根据应急演练目的、内容和形式可选择编制应急演练脚本，控制应急演练时间进程，对应急演练场景和响应程序进行详细说明，一般采用表格形式，以应急演练流程的各关键节点为骨干，描述应急演练的场景、起止时间、执行人员、处置行动、指令与对白、适时选用的技术设备、视频画面与字幕、解说词等	
应急演练评估方案	组织应制定应急演练评估方案，通过观察、体验和记录演练活动，比较应急演练实际效果与目标之间的差异，总结应急演练成效和不足的过程	

续表

控制项	网络安全事件应急演练的遵从要求	对应条款
应急演练评估方案	组织应根据应急演练场景、流程中的关键节点与处置工作要点，研究确定应急演练评估的考核要点、评估标准和方法，制定评估工作方案。评估工作方案主要内容包括：应急演练目标、应急演练场景清单及说明、评估人员组织结构与职责、评估人员位置、评估表格及相关工具、通信联络方式等	
应急演练保障措施	组织应提供应急演练人员、技术、物质、经费，以及安全保障措施	
3. 网络安全事件应急演练实施阶段		
安全事件模拟	组织应通过现象模拟或机理模拟的方式在应急演练中模拟网络安全事件	
应急演练执行	组织应确保网络安全事件应急演练具体操作与真实安全事件应急处理相同。具体步骤分为先期处置、现场处置、后期处置三个阶段	
演练过程与结果记录	组织应在应急演练实施过程中安排专门人员，采用文字、摄影、摄像、录音和工具记录等手段，全程采集应急演练相关资料	
演练结果与过程评估	<p>组织应从以下六方面对网络安全事件应急演练的效果进行评估：</p> <p>应急演练模拟现场的真实度</p> <p>依据相关专家及参加应急演练人员的打分，对模拟现场的真实度进行评价。</p> <p>应急响应时间</p> <p>先期响应时间：事件发生到开始实施先期处置的时间。</p> <p>先期处置时间：完成先期处置的时间。</p> <p>现场处置时间：完成现场处置的时间。</p> <p>恢复效果评价</p> <p>按照业务恢复要求的 RPO 和 RTO 时间，与实际完成的 RPO 和 RTO 时间进行对比判断恢复是否满足要求。</p> <p>应急预案质量评价</p> <p>评价应急预案在安全事件应急处理中的正确性、完善程度、细致程度。</p> <p>应急组织的分工协作评价</p> <p>评价应急组织的岗位设置、各岗位的分工、各岗位之间协作关系的合理性。</p> <p>组织成员的应急处置能力评价</p> <p>评价各岗位人员的突发事件判断能力、应急处置技术水平、手段及工具的熟练程度</p>	

续表

控制项	网络安全事件应急演练的遵从要求	对应条款
4. 网络安全事件应急演练改进阶段		
具体措施	组织应在应急演练结束后，根据应急演练评估报告、总结报告提出的问题和建议对应急管理工作（包括应急演练工作）进行持续改进。  组织应督促相关部门和人员，制订整改计划，明确整改目标，制定整改措施，落实整改资金，并应跟踪督查整改情况。  组织应按照改进计划，及时采取措施，在规定时间内完成各项改进工作任务，包括修改完善应急预案、对应急物资装备更新、有针对性地进行人员教育培训等	

四、监督管理与法律责任

《网络安全法》第八条规定，国家网信部门负责统筹协调网络安全工作和相关监督管理工作。国务院电信主管部门、公安部门和其他有关机关依照本法和有关法律、行政法规的规定，在各自职责范围内负责网络安全保护和监督管理工作。县级以上地方人民政府有关部门的网络安全保护和监督管理职责，按照国家有关规定确定。第三十九条第二款规定，国家网信部门应当统筹协调有关部门对关键信息基础设施的安全保护采取下列措施：（二）定期组织关键信息基础设施的运营者进行网络安全应急演练，提高应对网络安全事件的水平和协同配合能力。第五十三条规定，国家网信部门协调有关部门建立健全网络安全风险评估和应急工作机制，制定网络安全事件应急预案，并定期组织演练。负责关键信息基础设施安全保护工作的部门应当制定本行业、本领域的网络安全事件应急预案，并定期组织演练。由此可见，国家网信部门负责统筹协调网络安全应急演练的组织和实施，负责关键信息基础设施安全保护工作的部门负责本行业、本领域网络安全应急演练的组织和具体实施。

在法律责任方面，针对关键信息基础设施的运营者不履行《网络安全法》第三十四条第四款规定的网络安全保护义务，没有按照有关规定定期进行网络安全事件应急演练的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。

## 第八节 网络安全监督管理约谈措施

### 一、《网络安全法》相关规定及释义

《网络安全法》第五十六条对约谈制度进行了明确规定，省级以上人民政府有关部门在履行网络安全监督管理职责中，发现网络存在较大安全风险或者发生安全事件的，可以按照规定的权限和程序对该网络的运营者的法定代表人或者主要负责人进行约谈。网络运营者应当按照要求采取措施，进行整改，消除隐患。

#### （一）约谈的法律效力

关于《网络安全法》第五十六条规定的约谈制度，在全国人大法工委经济法室直接参与本法起草制定工作的人员编写的《中华人民共和国网络安全法释义》中被认成一种行政指导行为，具有警示、告诫、督促履行义务和教育指导等功能。但由于本条规定了“网络运营者应当按照要求采取措施，进行整改，消除隐患”，释义中又提出：“被约谈对象无正当理由不接受约谈，不接受整改意见或者不落实整改承诺的，约谈部门应当采取进一步的监管和追责措施。”似乎又延续了“约谈十条”（即《互联网新闻信息服务单位约谈工作规定》）的思路，承认了约谈的强制力<sup>①</sup>。

#### （二）约谈的主体和对象

监管部门如果因为约谈的柔性和执法成本低风险性而随意开展约谈，可能会影响企业的正常经营。被监管部门约谈，哪怕本质上不涉及违法行为，也可能影响企业声誉和形象。因此，监管部门要认识到约谈的严肃性，避免随意开展约谈、随意公开约谈信息等。《网络安全法》第五十六条将约谈的主体限定为“省级以上人民政府有关部门”体现了审慎的精神。另外，考虑到履行网络安全监督管理职责的部门涉及网信部门、工信部门、公安部门、关键信息基础设施的有关行业主

---

<sup>①</sup> 杨合庆. 中华人民共和国网络安全法释义[M]. 中国民主法治出版社, 2017.

管或监管部门等，在实践中还应当避免重复约谈。

约谈对象是网络运营者的法定代表人或者主要负责人，约谈主体可以根据情况确定约谈法定代表人或者主要负责人，为达到充分沟通的效果，可以允许法定代表人或主要负责人带本企业相关人员参加约谈。

### （三）约谈的程序

《网络安全法》第五十六条中强调，约谈要按照“规定的权限和程序”进行。目前对此尚无详细规定，但考虑到目前国家网信办已经出台的针对互联网新闻信息服务单位的“约谈十条”，《网络安全法》第五十六条规定的约谈在实践中可能按照“约谈十条”规定的程序执行。例如，应当提前告知约谈事由，并约定时间、地点和参加人员等。实施约谈时，应当由两名以上执法人员参加，主动出示证件，并记录约谈情况。

## 二、网络安全监督管理约谈措施的制度概述

约谈制度是指上级管理部门对未履行或未全面正确履行职责、未按时完成重要工作任务的下级组织或监管对象所进行的问责谈话制度。约谈制度首创于我国税务系统，迄今已广泛运用于工商、土地、社保、环保、安全生产、食品安全、消费维权、价格等领域。

### （一）约谈的概念及其适用范围

约谈作为一种问责谈话制度，分为两种类型：一种是上级行政机关约谈履职不力的下级行政机关负责人，另一种是行政机关约谈企业等被监管对象。约谈在我国自2003年税务系统首创后，经过十多年的发展，在工商、环保等领域也开始应用，并且相关的许多法规、规章、规范性文件中对约谈都进行了规定。

目前，规定约谈措施的法律包括《水污染防治法》、《大气污染防治法》、《境外非政府组织境内活动管理法》、《食品安全法》、《网络安全法》，都是2015年以来制定或修改的法律。其中，《水污染防治法》和《大气污染防治法》规定的约谈是行政机关之间的约谈。《水污染防治法》第二十条第五款规定：对超过重点水污

染物排放总量控制指标或者未完成水环境质量改善目标的地区，省级以上人民政府环境保护主管部门应当会同有关部门约谈该地区人民政府的主要负责人，并暂停审批新增重点水污染物排放总量的建设项目的环评文件。约谈情况应当向社会公开。《大气污染防治法》也做了类似规定。《境外非政府组织境内活动管理法》第四十一条规定，公安机关履行监督管理职责，发现涉嫌违反本法规定行为的，可以约谈境外非政府组织代表机构的首席代表以及其他负责人。《食品安全法》第一百一十四条规定，食品生产经营过程中存在食品安全隐患，未及时采取措施消除的，县级以上人民政府食品药品监督管理部门可以对食品生产经营者的法定代表人或者主要负责人进行责任约谈。食品生产经营者应当立即采取措施，进行整改，消除隐患。责任约谈情况和整改情况应当纳入食品生产经营者食品安全信用档案。

在网络安全领域，监管部门也曾多次对网络服务者进行约谈。例如，2010年爆发的“3Q大战”，工信部约谈了两个企业的负责人，在短时间内恢复了QQ软件和360产品的兼容。为了治理在提供互联网新闻信息服务过程中存在的违法转载新闻信息、传播淫秽色情信息、传播谣言，以及散布暴力、恐怖、诈骗等违法行为问题，国家网信办和北京等地网信办已尝试在依法处罚之外，通过约谈一些违法情节严重的互联网新闻信息服务单位，督促其采取有效措施进行整改。2015年，国家网信办及北京市网信办约谈了网易和新浪。2015年4月，国家网信办发布《互联网新闻信息服务单位约谈工作规定》（约谈十条），推动约谈工作进一步程序化、规范化。

## （二）约谈的法律性质

约谈体现了柔性执法精神，一定程度上可以缓解行政机关和被监管对象的紧张关系，有效避免冲突和矛盾，降低监管成本，提高监管效率。但行政机关对被监管对象的约谈性质如何定位，尚且存在不同认识。有的认为，约谈制度是行政指导或类行政指导行为，因为约谈具有双向互动性，行政主体在谈话中必然要听取行政相对人的意见，了解情况，提供警示、指导。有的认为，约谈制度是一种行政行为，具有强制性。本书认为，目前关于约谈制度的规定比较分散，不同领域的约谈制度在适用对象、约谈内容等方面存在较大差异，因此，对约谈的性质



不宜一概而论，要结合约谈内容、约谈对企业的影响等确定其性质。

对于监管部门来讲，如果将约谈定性为不具有强制力的行政指导行为，则可以降低监管部门被提起行政诉讼的风险。如果约谈措施是针对可能存在的风险，和企业交流信息、向企业提示风险，并没有通过强制手段给企业施加义务，则将其定性为行政指导是合适的。以价格领域的约谈为例，国家发展和改革委员会价格司（以下简称“国家发改委价格司”）有关负责人表示，约谈是一种沟通方式，不是行政干预，更谈不上干涉企业定价自主权，其主要目的是通过交流情况，沟通信息，引导企业更好地行使定价权，提醒经营者遵守国家相关法律法规和政策，自觉规范价格行为。

但如果在约谈中认定企业违法、责令企业改正等，就涉及对企业实体权利的干预，可能被认为因带有强制性而不属于单纯的行政指导范畴。例如，“约谈十条”第二条规定：本规定所称约谈，是指国家互联网信息办公室、地方互联网信息办公室在互联网新闻信息服务单位发生严重违法违规情形时，约见其相关负责人，进行警示谈话、指出问题、责令整改纠正的行政行为。

### （三）约谈的法律效力

《网络安全法》没有明确规定被约谈人是否有权拒绝参加约谈。“约谈十条”第九条规定：国家互联网信息办公室、地方互联网信息办公室履行约谈职责时，互联网新闻信息服务单位应当予以配合，不得拒绝、阻挠。但从实际操作角度来看，企业法定代表人或主要负责人拒绝参加约谈的，监管部门无权强制其参加约谈。

约谈很重要的一个功能就是信息沟通。如果企业不重视约谈，则不利于建立与监管部门的顺畅沟通机制，对企业发展也是不利的。即使形式上没有任何强制力的约谈，在实践中企业一般都非常重视，以各种形式配合约谈工作。例如，国家发改委价格司有关负责人就提到，大多数被约谈的企业“愿意主动承担社会责任，为稳定物价做出贡献。部分准备调价的企业要么推迟了调价时间，要么决定通过企业内部技术进步和提高劳动生产率，消化一部分成本上升因素。被约谈的一些行业协会和相关企业还发出了倡议书，承诺自觉遵守国家价格法律法规”。

应当看到，即使监管部门未采取干预措施，约谈也会对企业产生一定影响。例如，“约谈十条”第八条规定：国家互联网信息办公室、地方互联网信息办公室可将与互联网新闻信息服务单位的约谈情况向社会公开。约谈情况记入互联网新

闻信息服务单位日常考核和年检档案。

三、典型案例

“BOSS 直聘”是一款手机招聘 APP，属于北京华品博睿网络技术有限公司。该软件自 2014 年 7 月上线以来，一直宣称“去猎头化、中介化，是一款让职场 BOSS 与求职者在线聊天、加快面试的免费招聘手机软件”。2017 年 7 月 14 日，毕业于东北大学的李某的尸体在天津市静海区 G104 国道旁水坑里被发现。8 月 14 日，经天津警方证实，李文星系误入“蝶蓓蕾”传销团伙后死亡。

8 月 9 日，北京市网信办、天津市网信办开展联合执法专项行动，就“BOSS 直聘”发布违法违规信息、用户管理出现重大疏漏等问题，依法联合约谈“BOSS 直聘”（京 ICP 备 14013441 号）法人，并下达行政执法检查记录，责令网站立即整改。

四、网络安全监督管理约谈措施的法规遵从框架

网络安全监督管理约谈措施的法规遵从框架如表 7-15 所示。

表 7-15 网络安全监督管理约谈措施的法规遵从框架

法律名称	法律条款	法律规定
《网络安全法》	第五十六条	省级以上人民政府有关部门在履行网络安全监督管理职责中，发现网络存在较大安全风险或者发生安全事件的，可以按照规定的权限和程序对该网络的运营者的法定代表人或者主要负责人进行约谈。网络运营者应当按照要求采取措施，进行整改，消除隐患
《互联网新闻信息服务单位约谈工作规定》	第一条	为了进一步推进依法治网，促进互联网新闻信息服务单位依法办网、文明办网，规范互联网新闻信息服务，保护公民、法人和其他组织的合法权益，营造清朗网络空间，根据《互联网信息服务管理办法》、《互联网新闻信息服务管理规定》和《国务院关于授权国家互联网信息办公室负责互联网信息内容管理工作的通知》，制定本规定
	第二条	国家互联网信息办公室、地方互联网信息办公室建立互联网新闻信息服务单位约谈制度。 本规定所称约谈，是指国家互联网信息办公室、地方互联网信息办公室在互联网新闻信息服务单位发生严重违法违规情形时，约见其相关负责人，进行警示谈话、指出问题、责令整改纠正的行政行为

续表

法律名称	法律条款	法律规定
《互联网新闻信息服务单位约谈工作规定》	第三条	地方互联网信息办公室负责对本行政区域内的互联网新闻信息服务单位实施约谈，约谈情况应当及时向国家互联网信息办公室报告。 对存在重大违法情形的互联网新闻信息服务单位，由国家互联网信息办公室单独或联合属地互联网信息办公室实施约谈
	第四条	互联网新闻信息服务单位有下列情形之一的，国家互联网信息办公室、地方互联网信息办公室可对其主要负责人、总编辑等进行约谈： （一）未及时处理公民、法人和其他组织关于互联网新闻信息服务的投诉、举报情节严重的； （二）通过采编、发布、转载、删除新闻信息等谋取不正当利益的； （三）违反互联网用户账号名称注册、使用、管理相关规定情节严重的； （四）未及时处置违法信息情节严重的； （五）未及时落实监管措施情节严重的； （六）内容管理和网络安全制度不健全、不落实的； （七）网站日常考核中问题突出的； （八）年检中问题突出的； （九）其他违反相关法律法规规定需要约谈的情形
	第五条	国家互联网信息办公室、地方互联网信息办公室对互联网新闻信息服务单位实施约谈，应当提前告知约谈事由，并约定时间、地点和参加人员等。 国家互联网信息办公室、地方互联网信息办公室实施约谈时，应当由两名以上执法人员参加，主动出示证件，并记录约谈情况
	第六条	国家互联网信息办公室、地方互联网信息办公室通过约谈，及时指出互联网新闻信息服务单位存在的问题，并提出整改要求。 互联网新闻信息服务单位应当及时落实整改要求，依法提供互联网新闻信息服务
	第七条	国家互联网信息办公室、地方互联网信息办公室应当加强对互联网新闻信息服务单位的监督检查，并对其整改情况进行综合评估，综合评估可以委托第三方开展。 互联网新闻信息服务单位未按要求整改，或者经综合评估未达到整改要求的，将依照《互联网信息服务管理办法》、《互联网新闻信息服务管理规定》的有关规定给予警告、罚款、责令停业整顿、吊销许可证等处罚；互联网新闻信息服务单位被多次约谈仍然存在违法行为的，依法从重处罚
	第八条	国家互联网信息办公室、地方互联网信息办公室可将与互联网新闻信息服务单位的约谈情况向社会公开。 约谈情况记入互联网新闻信息服务单位日常考核和年检档案
	第九条	国家互联网信息办公室、地方互联网信息办公室履行约谈职责时，互联网新闻信息服务单位应当予以配合，不得拒绝、阻挠

续表

法律名称	法律条款	法律规定
《互联网信息服务内容管理行政执法程序规定》	第三十五条	互联网信息服务内容管理部门对互联网信息服务提供者违法行为做出行政处罚决定前，可以根据有关规定对其实施约谈，谈话结束后制作《执法约谈笔录》（格式见附件 12）
《证券期货业信息安全保障管理办法》	第五十条	核心机构和经营机构违反本办法规定，中国证监会可以视情节，依法对其采取责令改正、监管谈话、出具警示函、公开谴责、责令定期报告、责令处分有关人员、撤销任职资格、暂停或者限制证券期货经营业务活动等措施；情节严重的，给予警告、罚款

第九节 网络通信临时管制

一、《网络安全法》相关规定及释义

《网络安全法》第五十八条规定：因维护国家和社会公共秩序，处置重大突发社会安全事件的需要，经国务院决定或者批准，可以在特定区域对网络通信采取限制等临时措施。

（一）网络通信临时管制的必要性

网络的开放性一方面带来信息交流与共享的自由，另一方面也造成违法信息的泛滥和存在网络滥用行为。分裂国家的信息对国家稳定和国家政权造成严重影响；恐怖主义、极端主义等势力利用网络煽动、策划、组织和实施暴力恐怖活动，直接威胁人民生命财产安全、社会秩序；网络谣言、颓废文化和淫秽、暴力、迷信等违背社会主义核心价值观的有害信息侵蚀青少年身心健康，败坏社会风气，误导价值取向，危害文化安全。除此之外，个别国家强化网络威慑战略，加剧网络空间军备竞赛，也为世界和平与网络社会带来新的挑战。在信息快速传播、网络犯罪成本低而危害结果重大的情况下，对于这些信息与违法行为的及时、有效管制就显得极为重要。

网络通信临时管制，包括网络通信限制以及其他措施，例如，限制或禁止使用电子邮件系统传输相关信息，限制或停止使用即时通信软件，关闭相关网站，

封堵部分网络路由,屏蔽消息,限制或停止互联网服务等。网络通信临时管制措施,是应对网络安全突发事件、网络违法行为特别是网络犯罪、恐怖主义的重要措施。《国家安全法》第二十五条规定:国家建设网络与网络安全保障体系,提升网络与网络安全保护能力,加强网络和信息技术的创新研究和开发应用,实现网络和信息核心技术、关键基础设施和重要领域信息系统及数据的安全可控;加强网络管理,防范、制止和依法惩治网络攻击、网络入侵、网络窃密、散布违法有害信息等网络违法犯罪行为,维护国家网络空间主权、安全和发展利益。《中华人民共和国突发事件应对法》(以下简称《突发事件应对法》)第四十八条规定:突发事件发生后,履行统一领导职责或者组织处置突发事件的人民政府应当针对其性质、特点和危害程度,立即组织有关部门,调动应急救援队伍和社会力量,依照本章的规定和有关法律、法规、规章的规定采取应急处置措施。第四十九条规定的应急处置措施中包括了禁止或者限制使用有关设备、设施。《反恐怖主义法》第六十一条规定,恐怖事件发生后,负责应对处置的反恐怖主义工作领导机构可以决定由有关部门和单位在特定区域内实施互联网、无线电、通信管制。

## (二) 网络通信临时管制措施的实施条件

### 1. 目的在于维护国家和社会公共秩序

由于网络通信临时管制措施一旦实施,会对大量用户的正常通信、访问网站产生影响,所以必须对网络通信临时管制措施进行严格限制。实施网络通信临时管制的目的,必须是基于维护国家和社会公共秩序,处置重大突发社会安全事件的需要,除此之外禁止实施网络通信临时管制措施。对网络通信临时管制措施进行必要的限制,也是维护国家和社会稳定的必然要求。

《网络安全法》第五十八条中使用的“重大突发社会安全事件”概念,涉及与《突发事件应对法》等相关规定的衔接问题,在实行中应当引起关注。根据《突发事件应对法》的规定,突发事件是指突然发生,造成或者可能造成严重社会危害,需要采取应急处置措施予以应对的自然灾害、事故灾难、公共卫生事件和社会安全事件。《突发事件应对法》将自然灾害、事故灾难、公共卫生事件分为特别重大、重大、较大和一般四级,未明确对社会安全事件的分级。《重大、特别重大突发公

共事件分级标准（试行）》规定了六类“社会安全事件”，包括群体性事件、金融突发事件、涉外突发事件、影响市场稳定的突发事件、恐怖袭击事件和刑事案件。其中，界定了群体性事件、金融突发事件、涉外突发事件、影响市场稳定的突发事件和刑事案件除恐怖袭击事件的“特别重大”和“重大”认定标准，对于恐怖袭击事件，未进一步区分“特别重大”和“重大”的标准认定。因此，不能机械理解《网络安全法》使用的“重大突发社会安全事件”概念，其应涵盖《重大、特别重大突发公共事件分级标准（试行）》中划定的“重大”和“特别重大”社会安全事件，也包括了恐怖袭击等在相关细则中没有进一步明确区分“重大”和“特别重大”标准的突发社会安全事件。

## 2. 需要经国务院决定或者批准

对于需要采取网络通信临时管制措施，符合条件的，国务院可以直接决定采取关闭相关网站，封堵部分网络路由，屏蔽消息，限制或停止互联网服务等网络通信临时管制措施，也可以由地方政府、相关部门等向国务院提出申请，经国务院批准后采取上述网络通信临时管制措施。因此，无论是上述哪种情况，经过国务院决定或者批准都是法律规定的必经程序。

## 3. 必须在特定区域实施

实践中，网络通信临时管制措施的实施可能给网络运营者和使用者带来不便，甚至造成损失，这是维护国家和社会公共利益所要承担的义务和履行的责任，是面对国家和社会利益时对个人利益进行的必要限制和剥夺，但这并不意味着国家可以任意地施加这种限制。由于网络通信临时管制措施针对的是特定区域的特定事件，所以实施范围也仅限于该特定区域，对于其他区域，禁止实施网络通信临时管制措施。

## （三）网络通信临时管制措施的解除

网络通信临时管制措施的实施具有一定的期限性和临时性，其实施基于网络安全事件的动态，在事件持续的过程中，应当综合考虑突发社会安全事件的性质、严重程度、影响范围等因素，尽可能降低对社会正常秩序的影响。当事件结束后，网络通信临时管制措施的实施条件消除，网络运营者必须立即开通相应的通信和

网络服务，恢复正常的通信和网络运营，以使个人利益受限制或受剥夺的状态尽快得到恢复。

值得注意的是，在实行网络通信临时管制措施的过程中，网络运营者和使用者可以事先采取合理措施尽可能避免损失，例如，在网络服务合同中将此种情形列为己方的免责条款。此外，采取网络通信临时管制措施的过程中，由于网络运营者实施了关闭、封锁网络等措施，使得其在此期间部分业务无法正常运营，由此造成的这部分运营损失，其有权依据行政补偿制度，要求国家给予适当的补偿。

二、典型案例

和田位于新疆维吾尔自治区最南端，是暴恐事件多发地区。2014 年 5 月 23 日，新疆维吾尔自治区曾召开会议，决定结合新疆当前严峻的反恐维稳形势，从 5 月 23 日起到 2015 年 6 月，以新疆为主战场启动严打暴力恐怖活动专项行动。2014 年 5 月 27 日，新疆和田地区严厉打击暴力恐怖活动专项行动指挥部发布《关于对部分即时通信工具临时管制的通告》，称将从 5 月 28 日零时起，对新疆和田地区的微信和 QQ 先行采取临时管制措施。此次临时管制的目的是切断境内外“三股势力”（暴力恐怖势力、民族分裂势力、宗教极端势力）勾连、宣传、造谣、煽动渠道。此次限制措施仅针对部分即时通信工具（微信、QQ），不影响用户正常上网、通话、短信功能的使用。

三、网络通信临时管制的法规遵从框架

网络通信临时管制的法规遵从框架如表 7-16 所示。

表 7-16 网络通信临时管制的法规遵从框架

法律名称	法律条款	法律规定
《反恐怖主义法》	第六十一条	恐怖事件发生后，负责应对处置的反恐怖主义工作领导机构可以决定由有关部门和单位采取下列一项或者多项应对处置措施：  （四）在特定区域内实施互联网、无线电、通信管制

续表

法律名称	法律条款	法律规定
《网络安全法》	第五十八条	因维护国家和社会公共秩序，处置重大突发社会安全事件的需要，经国务院决定或者批准，可以在特定区域对网络通信采取限制等临时措施

第十节 突发事件应对

一、《网络安全法》相关规定及释义

网络安全事件与突发事件、生产安全事故存在一定的交叉，有的网络安全事件可能属于或导致突发事件、生产安全事故。不同事件或事故的处理主管部门、处理程序、处理方式等存在差异，如果对同一事件或事故，不同部门依据不同法律要求介入，则会引起不必要的混乱，影响对事件或事故的有效处理。为解决这一问题，《网络安全法》第五十七条规定：因网络安全事件，发生突发事件或者生产安全事故的，应当依照《突发事件应对法》、《中华人民共和国安全生产法》（以下简称《安全生产法》）等有关法律、行政法规的规定处置。

（一）网络安全事件、突发事件和生产安全事故的关系

根据《国家网络安全事件应急预案》的规定，网络安全事件是指由于人为原因、软硬件缺陷或故障、自然灾害等，对网络和信息系统或者其中的数据造成危害，对社会造成负面影响的事件，可分为有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障、灾害性事件和其他事件。级别上分为四级：特别重大、重大、较大和一般。

根据《突发事件应对法》第三条的规定，突发事件是指突然发生，造成或者可能造成严重社会危害，需要采取应急处置措施予以应对的自然灾害、事故灾害、公共卫生事件和社会安全事件。自然灾害、事故灾害、公共卫生事件分为特别重大、重大、较大和一般四级。

生产安全事故，是指生产经营活动中发生的造成人身伤亡或财产损失的事故。



国务院 2007 年颁布的《生产安全事故报告和调查处理条例》将生产安全事故分为四级：特别重大事故，是指造成 30 人以上死亡，或者 100 人以上重伤（包括急性工业中毒，下同），或者 1 亿元以上直接经济损失的事故；重大事故，是指造成 10 人以上 30 人以下死亡，或者 50 人以上 100 人以下重伤，或者 5 000 万元以上 1 亿元以上直接经济损失的事故；较大事故，是指造成 3 人以上 10 人以下死亡，或者 10 人以上 50 人以下重伤，或者 1 000 万元以上 5 000 万元以下直接经济损失的事故；一般事故，是指造成 3 人以下死亡，或者 10 人以下重伤，或者 1 000 万元以下直接经济损失的事故。

## （二）突发事件处置

### 1. 突发事件处置机制

- 一般采取属地管理

突发事件处置一般采取属地管理，由突发事件发生地人民政府负责处置。县级人民政府对本行政区域内突发事件的应对工作负责。涉及两个以上行政区域的，由有关行政区域共同的上一级人民政府负责，或者由各有关行政区域的上一级人民政府共同负责。突发事件发生地县级人民政府不能消除或者不能有效控制突发事件引起的严重社会危害的，应当及时向上级人民政府报告。上级人民政府应当及时采取措施，统一领导应急处置工作。法律、行政法规规定由国务院有关部门对突发事件的应对工作负责的，从其规定；地方人民政府应当积极配合并提供必要的支持。

- 政府内部工作机制

国务院在总理领导下研究、决定和部署特别重大突发事件的应对工作，根据实际情况需要，设立国家突发事件应急指挥机构，必要时可以派出工作组指导有关工作。

县级以上地方各级人民政府设立由本级人民政府主要负责人、相关部门负责人、驻当地中国人民解放军和中国人民武装警察部队有关负责人组成的突发事件应急指挥机构；根据实际工作需要，设立相关类别突发事件应急指挥机构。

### 2. 突发事件处置措施

自然灾害、事故灾难或者公共卫生事件发生后，履行统一领导职责的人民政府可以采取下列一项或者多项应急处置措施：①组织营救和救治受害人员，疏散、

撤离并妥善安置受到威胁的人员以及采取其他救助措施；②迅速控制危险源，标明危险区域，封锁危险场所，划定警戒区，实行交通管制以及其他控制措施；③立即抢修被损坏的交通、通信、供水、排水、供电、供气、供热等公共设施，向受到危害的人员提供避难场所和生活必需品，实施医疗救护和卫生防疫以及其他保障措施；④禁止或者限制使用有关设备、设施，关闭或者限制使用有关场所，中止人员密集的活动或者可能导致危害扩大的生产经营活动以及采取其他保护措施；⑤启用本级人民政府设置的财政预备费和储备的应急救援物资，必要时调用其他急需物资、设备、设施、工具；⑥组织公民参加应急救援和处置工作，要求具有特定专长的人员提供服务；⑦保障食品、饮用水、燃料等基本生活必需品的供应；⑧依法从严惩处囤积居奇、哄抬物价、制假售假等扰乱市场秩序的行为，稳定市场价格，维护市场秩序；⑨依法从严惩处哄抢财物、干扰破坏应急处置工作等扰乱社会秩序的行为，维护社会治安；⑩采取防止发生次生、衍生事件的必要措施。

社会安全事件发生后，则组织处置工作的人民政府应当立即组织有关部门并由公安机关针对事件的性质和特点，依照有关法律、行政法规和国家其他有关规定，采取下列一项或者多项应急处置措施：①强制隔离使用器械相互对抗或者以暴力行为参与冲突的当事人，妥善解决现场纠纷和争端，控制事态发展；②对特定区域内的建筑物、交通工具、设备、设施以及燃料、燃气、电力、水的供应进行控制；③封锁有关场所、道路，查验现场人员的身份证件，限制有关公共场所内的活动；④加强对易受冲击的核心机关和单位的警卫力量，在国家机关、军事机关、国家通讯社、广播电台、电视台、外国驻华使领馆等单位附近设置临时警戒线；⑤法律、行政法规和国务院规定的其他必要措施。

严重危害社会治安秩序的事件发生时，公安机关应当立即依法出动警力，根据现场情况依法采取相应的强制性措施，尽快使社会秩序恢复正常。

发生突发事件，严重影响国民经济正常运行时，国务院或者国务院授权的有关主管部门可以采取保障、控制等必要的应急措施，保障人民群众的基本生活需要，最大限度地减轻突发事件的影响。

### 3. 突发事件的应对

(1) 人民政府。履行统一领导职责或者组织处置突发事件的人民政府，必要

时可以向单位和个人征用应急救援所需设备、设施、场地、交通工具和其他物资，请求其他地方人民政府提供人力、物力、财力或者技术支援，要求生产、供应生活必需品和应急救援物资的企业组织生产、保证供给，要求提供医疗、交通等公共服务的组织提供相应的服务。还应当组织协调运输经营单位，优先运送处置突发事件所需物资、设备、工具、应急救援人员和受到突发事件危害的人员。除了对物资等的安排，还应当按照有关规定统一、准确、及时发布有关突发事件事态发展和应急处置工作的信息。

(2) 居民委员会、村民委员会和其他组织。突发事件发生地的居民委员会、村民委员会和其他组织应当按照当地人民政府的决定、命令，进行宣传动员，组织群众开展自救和互救，协助维护社会秩序。

(3) 突发事件发生单位。受到发生事故灾难的单位，应当立即组织本单位应急救援队伍和工作人员营救受害人员，疏散、撤离、安置受到威胁的人员，控制危险源，标明危险区域，封锁危险场所，并采取其他防止危害扩大的必要措施，同时向所在地县级人民政府报告；对因本单位的问题引发的或者主体是本单位人员的社会安全事件，有关单位应当按照规定上报情况，并迅速派出负责人赶赴现场开展劝解、疏导工作。

(4) 其他单位。突发事件发生地的其他单位应当服从人民政府发布的决定、命令，配合人民政府采取的应急处置措施，做好本单位的应急救援工作，并积极组织人员参加所在地的应急救援和处置工作。

(5) 事故发生地公民。突发事件发生地的公民应当服从人民政府、居民委员会、村民委员会或者所属单位的指挥和安排，配合人民政府采取的应急处置措施，积极参加应急救援工作，协助维护社会秩序。

#### 4. 突发事件应对的特殊情况

(1) 发生特别重大突发事件，对人民生命财产安全、国家安全、公共安全、环境安全或者社会秩序构成重大威胁，采取本法和其他有关法律、法规、规章规定的应急处置措施不能消除或者有效控制、减轻其严重社会危害，需要进入紧急状态的，由全国人大常委会或者国务院依照宪法和其他有关法律规定的权限和程序决定。

(2) 紧急状态期间采取的非常措施，依照有关法律规定执行或者由全国人大

常委会另行规定。

(3) 突发事件的威胁和危害得到控制或者消除后，履行统一领导职责或者组织处置突发事件的人民政府应当停止执行依照本法规定采取的应急处置措施，同时采取或者继续实施必要措施，防止发生自然灾害、事故灾难、公共卫生事件的次生、衍生事件或者重新引发社会安全事件。

二、典型案例

河北省遵化市职教中心项目承建企业在拖欠农民工工资 6 年之久后，仍然不予支付。2013 年临近春节之际，100 多名公民共为了讨回工资，无奈集结在遵化市政府门口下跪。对于百余名公民共的下跪，市政府竟然置之不理。这件事于 2013 年 1 月 6 日被发布在某论坛上，进而引发大量网民的关注。1 月 13 日，腾讯新闻也转载了配图新闻。经过事件的不断发酵，2013 年 1 月 22 日，中央电视台《东方时空》栏目组播出节目，对事件中所涉该市劳动监察大队个别工作人员粗暴的接访态度进行曝光。毫无疑问，在该突发事件中，遵化市政府并未对事件做出积极有效的应对和处置，而是置之不理，任由其发展，最后造成更大的网络舆论。

三、突发事件应对的法规遵从框架

突发事件应对的法规遵从框架如表 7-17 所示。

表 7-17 突发事件应对的法规遵从框架

法律名称	法律条款	法律规定
《网络安全法》	第五十七条	因网络安全事件，发生突发事件或者生产安全事故的，应当依照《突发事件应对法》、《安全生产法》等有关法律、行政法规的规定处置
《突发事件应对法》	第三条	本法所称突发事件，是指突然发生，造成或者可能造成严重社会危害，需要采取应急处置措施予以应对的自然灾害、事故灾难、公共卫生事件和社会安全事件
	第四十八条	突发事件发生后，履行统一领导职责或者组织处置突发事件的人民政府应当针对其性质、特点和危害程度，立即组织有关部门，调动应急救援队伍和社会力量，依照本章的规定和有关法律、法规、规章的规定采取应急处置措施

续表

法律名称	法律条款	法律规定
《突发事件应对法》	第四十九条	<p>自然灾害、事故灾难或者公共卫生事件发生后，履行统一领导职责的人民政府可以采取下列一项或者多项应急处置措施：</p> <p>（一）组织营救和救治受害人员，疏散、撤离并妥善安置受到威胁的人员以及采取其他救助措施；</p> <p>（二）迅速控制危险源，标明危险区域，封锁危险场所，划定警戒区，实行交通管制以及其他控制措施；</p> <p>（三）立即抢修被损坏的交通、通信、供水、排水、供电、供气、供热等公共设施，向受到危害的人员提供避难场所和生活必需品，实施医疗救护和卫生防疫以及其他保障措施；</p> <p>（四）禁止或者限制使用有关设备、设施，关闭或者限制使用有关场所，中止人员密集的活动或者可能导致危害扩大的生产经营活动以及采取其他保护措施；</p> <p>（五）启用本级人民政府设置的财政预备费和储备的应急救援物资，必要时调用其他急需物资、设备、设施、工具；</p> <p>（六）组织公民参加应急救援和处置工作，要求具有特定专长的人员提供服务；</p> <p>（七）保障食品、饮用水、燃料等基本生活必需品的供应；</p> <p>（八）依法从严惩处囤积居奇、哄抬物价、制假售假等扰乱市场秩序的行为，稳定市场价格，维护市场秩序；</p> <p>（九）依法从严惩处哄抢财物、干扰破坏应急处置工作等扰乱社会秩序的行为，维护社会治安；</p> <p>（十）采取防止发生次生、衍生事件的必要措施</p>
	第五十条	<p>社会安全事件发生后，组织处置工作的人民政府应当立即组织有关部门并由公安机关针对事件的性质和特点，依照有关法律、行政法规和国家其他有关规定，采取下列一项或者多项应急处置措施：</p> <p>（一）强制隔离使用器械相互对抗或者以暴力行为参与冲突的当事人，妥善解决现场纠纷和争端，控制事态发展；</p> <p>（二）对特定区域内的建筑物、交通工具、设备、设施以及燃料、燃气、电力、水的供应进行控制；</p> <p>（三）封锁有关场所、道路，查验现场人员的身份证件，限制有关公共场所内的活动；</p> <p>（四）加强对易受冲击的核心机关和单位的警卫力量，在国家机关、军事机关、国家通讯社、广播电台、电视台、外国驻华使领馆等单位附近设置临时警戒线；</p>

续表

法律名称	法律条款	法律规定
《突发事件应对法》	第五十条	<p>（五）法律、行政法规和国务院规定的其他必要措施。</p> <p>严重危害社会治安秩序的事件发生时，公安机关应当立即依法出动警力，根据现场情况依法采取相应的强制性措施，尽快使社会秩序恢复正常</p>
	第五十一条	<p>发生突发事件，严重影响国民经济正常运行时，国务院或者国务院授权的有关主管部门可以采取保障、控制等必要的应急措施，保障人民群众的基本生活需要，最大限度地减轻突发事件的影响</p>
	第五十二条	<p>履行统一领导职责或者组织处置突发事件的人民政府，必要时可以向单位和个人征用应急救援所需设备、设施、场地、交通工具和其他物资，请求其他地方人民政府提供人力、物力、财力或者技术支援，要求生产、供应生活必需品和应急救援物资的企业组织生产、保证供给，要求提供医疗、交通等公共服务的组织提供相应的服务。</p> <p>履行统一领导职责或者组织处置突发事件的人民政府，应当组织协调运输经营单位，优先运送处置突发事件所需物资、设备、工具、应急救援人员和受到突发事件危害的人员</p>
	第五十三条	<p>履行统一领导职责或者组织处置突发事件的人民政府，应当按照有关规定统一、准确、及时发布有关突发事件事态发展和应急处置工作的信息</p>
	第五十四条	<p>任何单位和个人不得编造、传播有关突发事件事态发展或者应急处置工作的虚假信息</p>
	第五十五条	<p>突发事件发生地的居民委员会、村民委员会和其他组织应当按照当地人民政府的决定、命令，进行宣传动员，组织群众开展自救和互救，协助维护社会秩序</p>
	第五十六条	<p>受到自然灾害危害或者发生事故灾难、公共卫生事件的单位，应当立即组织本单位应急救援队伍和工作人员营救受害人员，疏散、撤离、安置受到威胁的人员，控制危险源，标明危险区域，封锁危险场所，并采取其他防止危害扩大的必要措施，同时向所在地县级人民政府报告；对因本单位的问题引发的或者主体是本单位人员的社会安全事件，有关单位应当按照规定上报情况，并迅速派出负责人赶赴现场开展劝解、疏导工作。</p> <p>突发事件发生地的其他单位应当服从人民政府发布的决定、命令，配合人民政府采取的应急处置措施，做好本单位的应急救援工作，并积极组织人员参加所在地的应急救援和处置工作</p>

续表

法律名称	法律条款	法律规定
《突发事件应对法》	第五十七条	突发事件发生地的公民应当服从人民政府、居民委员会、村民委员会或者所属单位的指挥和安排，配合人民政府采取的应急处置措施，积极参加应急救援工作，协助维护社会秩序
	第七十六条	<p>国家加强生产安全事故应急能力建设，在重点行业、领域建立应急救援基地和应急救援队伍，鼓励生产经营单位和其他社会力量建立应急救援队伍，配备相应的应急救援装备和物资，提高应急救援的专业化水平。</p> <p>国务院安全生产监督管理部门建立全国统一的生产安全事故应急救援信息系统，国务院有关部门建立健全相关行业、领域的生产安全事故应急救援信息系统</p>
	第七十七条	县级以上地方各级人民政府应当组织有关部门制定本行政区域内特大生产安全事故应急救援预案，建立应急救援体系
	第七十八条	生产经营单位应当制定本单位生产安全事故应急救援预案，与所在地县级以上地方人民政府组织制定的生产安全事故应急救援预案相衔接，并定期组织演练
	第七十九条	<p>危险物品的生产、经营、储存单位以及矿山、金属冶炼、城市轨道交通运营、建筑施工单位应当建立应急救援组织；生产经营规模较小的，可以不建立应急救援组织，但应当指定兼职的应急救援人员。</p> <p>危险物品的生产、经营、储存、运输单位以及矿山、金属冶炼、城市轨道交通运营、建筑施工单位应当配备必要的应急救援器材、设备和物资，并进行经常性维护、保养，保证正常运转</p>
	第八十条	<p>生产经营单位发生生产安全事故后，事故现场有关人员应当立即报告本单位负责人。</p> <p>单位负责人接到事故报告后，应当迅速采取有效措施，组织抢救，防止事故扩大，减少人员伤亡和财产损失，并按照国家有关规定立即如实报告当地负有安全生产监督管理职责的部门，不得隐瞒不报、谎报或者迟报，不得故意破坏事故现场、毁灭有关证据</p>
	第八十一条	负有安全生产监督管理职责的部门接到事故报告后，应当立即按照国家有关规定上报事故情况。负有安全生产监督管理职责的部门和有关地方人民政府对事故情况不得隐瞒不报、谎报或者迟报
	第八十二条	有关地方人民政府和负有安全生产监督管理职责的部门的负责人接到生产安全事故报告后，应当按照生产安全事故应急救援预案的要求立即赶到事故现场，组织事故抢救

续表

法律名称	法律条款	法律规定
《安全生产法》	第八十二条	<p>参与事故抢救的部门和单位应当服从统一指挥，加强协同联动，采取有效的应急救援措施，并根据事故救援的需要采取警戒、疏散等措施，防止事故扩大和次生灾害的发生，减少人员伤亡和财产损失。</p> <p>事故抢救过程中应当采取必要措施，避免或者减少对环境造成的危害。</p> <p>任何单位和个人都应当支持、配合事故抢救，并提供一切便利条件</p>
《电信网络运行监督管理办法》	第三十条	<p>发生网络运行事故后，基础电信业务经营者有关人员应当立即报告本单位负责人。</p> <p>单位负责人接到事故报告后，应当迅速采取有效措施，组织抢修，防止事故扩大，减少社会影响和财产损失</p>
	第三十一条	<p>发生特别重大、重大事故后，基础电信业务经营者总部应当向工业和信息化部报告事故情况，同时其省级机构应当向相关省、自治区、直辖市通信管理局报告事故情况。</p> <p>发生较大事故后，基础电信业务经营者省级机构应当向相关省、自治区、直辖市通信管理局报告事故情况。</p> <p>发生一般事故后，基础电信业务经营者省级机构应当向相关省、自治区、直辖市通信管理局定期报送。</p> <p>发生网络运行事故后，任何单位和个人不得迟报、漏报、谎报或者瞒报</p>
	第三十二条	<p>网络运行事故报告分为口头报告、简要书面报告（格式见附件二）和专题书面报告（格式见附件三）三种。</p> <p>发生网络运行事故后，基础电信业务经营者总部及其省级机构应当在规定时限内向电信监管部门报告（具体报告时限见附件四）</p>
	第三十三条	<p>基础电信业务经营者上报的简要书面报告应当经本企业主管领导或主管部门领导认定，专题书面报告须经本企业主管领导认定</p>
	第三十四条	<p>事故的口头报告内容应当包括事故发生时间、地点、预计影响范围、事故原因的初步判断、已经或即将采取的措施。简要书面报告的内容应当包括事故发生时间、地点、影响范围、事故原因的初步判断、事故初步处理措施等。专题书面报告的内容应当包括事故发生时间、地点、影响范围、事故原因、责任认定、处理意见、防范措施等</p>
	第三十五条	<p>基础电信业务经营者应当认真总结经验教训，排除事故隐患，落实整改措施，并将对事故有关责任单位和责任人的处理意见，报相关电信监管部门</p>



# 安全认证、检测及风险评估

目前，我国网络安全形势异常严峻，物理安全、运行安全、数据安全、内容安全等层面都呈现高危状态，国家安全、社会稳定、企业发展、个人人权等相关法益也不同程度遭到威胁。风险社会的全球背景、攻击大于防御的残酷现实、风险加成的进一步催化，寻求态势感知下的主动防御成为必要和常态。网络安全认证、检测及风险评估制度是网络安全主动防御的关键和基础，它为降低网络风险，实施风险管理及风险控制提供直接的依据。2017 年 6 月 1 日生效施行的《网络安全法》全文一直贯穿着“保障法”的职能，第三条、第五条、第九条、第十七条、第二十三条、第二十六条、第三十八条、第三十九条、第五十五条等条文，从国家、网络运营者、协会组织等不同主体，对网络安全风险的预防做出了法律规定，明确了网络安全认证、检测和风险评估制度。网络运营者既是网络安全风险预防的重要力量，也是《网络安全法》主要遵从者。从经济学视角来看，网络运营者对《网络安全法》的有效法律遵从，以及网络安全风险有效预防便是其正外部性效应。因此，网络运营者如何履行《网络安全法》要求的网络安全认证、检测及风险评估的法定义务是本章的主要内容。

## 第一节 《网络安全法》相关规定及释义

网络（信息）安全是总体国家安全观体系中的重要组成，并与其他安全问

题相互交织并愈演愈烈，系当今时代的主要安全问题。风险社会的特性，以及对网络（信息）安全问题的立法，使我们必然遵从社会运行基本规律，实现网络（信息）安全的风险可控，而建构协同立体化的主动防御保障体系也变成网络安全立法的目的。《网络安全法》第三条对此做出了明确的立法回应——“建立健全网络安全保障体系”。

在主动防御的网络保全保障体系构建中，网络安全认证、检测和风险评估工作便成为至关重要的基础工作，在《网络安全法》中多处提及认证、检测、风险等，更有专门条文明确确立网络安全认证、检测和风险评估制度及相关要求，具体包括《网络安全法》第十七条、第二十三条、第二十六条、第三十八条、第三十九条等。

## 一、《网络安全法》第十七条的解读

《网络安全法》第十七条规定：国家推进网络安全社会化服务体系建设，鼓励有关企业、机构开展网络安全认证、检测和风险评估等安全服务。从立法职能视角审视，该条属于典型的促进型立法，这是我国近年来政府职能从管理型向服务型转变在网络安全领域的主要体现，其关键在于构建国家主导下的公众参与治理机制；从立法内容和立法技术视角解读，该条意在网络安全认证、检测和风险评估等安全服务体系的强调，即立法者意在表明网络安全认证、检测和风险评估等安全服务的极度重要性，否则不会以单独条文予以示明，更在于促进网络安全认证、检测和风险评估等安全服务行业的发展，吸纳社会力量。总之，该条为我国网络安全认证、检测和风险评估的安全服务行业的发展提供了指引，是立法先行的法治化体现。

但需要注意的是，该条可能被网络运营者错误解读，认为该条作为促进型立法不具有强制性。因为仅从该条法律规范进行文本解释，确属无法得出，网络安全运营者是否必须承担网络安全认证、检测和风险评估的强制义务。但对该条进行目的解释和系统解释便可清晰地发现，《网络安全法》要求网络运营者必须承担网络安全认证、检测和风险评估的强制义务。首先，我国网络安全形势十分严峻，尤其是受制于互联网关键资源支配不足引发的网络安全风险（即使我国已经正在

努力重塑全球网络治理体系，但根本格局尚未改变），为此，提升网络安全风险态势感知能力成为必然选择，也导致网络运营者必须承担相应的强制性义务，因为网络安全认证、检测和风险评估是网络安全风险预防的基础和关键。同时，通过对《网络安全法》文本的系统梳理也可以印证此观点。《网络安全法》第二十三条、第二十六条、第三十八条、第三十九条、第五十五条针对网络关键设备和网络安全专用产品、关键信息基础设施的运营者等可能涉及重大风险域的部分均做出了强制性规定。这也是为避免我国的网络运营者对《网络安全法》第十七条作为促进型立法不具有强制保障性的错误理解。当然，这也体现了我国《网络安全法》立法在网络安全认证、检测和风险评估等安全服务的立法中，为了增强全社会的防御力量，整体采用促进态势，但在事关国家安全和重大风险的网络安全风险域中采用重点保护的策略。

## 二、《网络安全法》第二十三条的解读

《网络安全法》第二十三条规定：网络关键设备和网络安全专用产品应当按照相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求后，方可销售或者提供。国家网信部门会同国务院有关部门制定、公布网络关键设备和网络安全专用产品目录，并推动安全认证和安全检测结果互认，避免重复认证、检测。该条是关于网络关键设备和网络安全专用产品的认证和安全检测的规定。

对网络关键设备和网络安全专用产品的认证和安全检测，是国际通行做法，是我国网络（信息）安全标准化建设的重要制度，也是对我国前期网络安全立法、实践的总结。在我国前期立法和网络安全实践中，已经有大量先例。例如，《中华人民共和国电信条例》（以下简称《电信条例》）、《中华人民共和国计算机信息系统安全保护条例》（以下简称《计算机信息系统安全保护条例》）、《中华人民共和国认证认可条例》（以下简称《认证认可条例》）等前期立法中就有大量的关于许可、安全认证、安全检测的规定。具体而言，依据《电信条例》，国务院电信主管部门建立了电信设备进网许可制度，并对电信终端设备、无线电通信设备、网间互联设备进行入网检测；依据《计算机信息系统安全保护条例》，国务院公安部门建立了信息安全专用产品销售许可制度，并对用于保护计算机信息系统安全的专

用硬件和软件产品进行安全功能检测；依据《认证认可条例》，国务院质检部门建立了信息安全产品认证制度，并实施信息安全产品认证。《网络安全法》作为网络安全领域的基本大法，将网络关键设备和网络安全专用产品的安全认证和检测制度专门予以确立，这充分表明了此制度的重要性。因此，对于网络运营者，尤其是网络关键设备和网络安全专用产品的销售者或提供者，应当全面、准确地理解该条文，尤其是该条文所要求的最低保障义务。

从网络关键设备和网络安全专用产品的销售者或提供者最低网络安全保护义务履行的视角对该条解读，需要关注以下问题。

### （一）“网络关键设备和网络安全专用产品”的认定

由于网络关键设备和网络安全专用产品的销售者或提供者将要承担网络安全认证或检测的积极义务，从运营成本视角来看，这将加大网络安全专用产品的销售者或提供者的运营费用；从法律合规视角来看，这将关系判定网络安全专用产品的销售者或提供者是否履行了网络安全最低保障义务结果；从网络安全风险控制实现视角来看，这将关系到重大网络风险项是否得以识别结果。为此，网络关键设备和网络安全专用产品的认定成为首要问题。

此条文规定国家网信部门会同国务院有关部门制定并公布网络关键设备和网络安全专用产品目录。2017年6月1日，在《网络安全法》正式实施的同日，为加强网络关键设备和网络安全专用产品安全管理，依据《网络安全法》，国家互联网信息办公室会同工业和信息化部、公安部、国家认证认可监督管理委员会已经共同制定了第一批《网络关键设备和网络安全专用产品目录》。这为“网络关键设备和网络安全专用产品”的认定提供了明确的指引。

但此时需要注意的一个问题是，在网络关键设备和网络安全专用产品目录继续制定和公布的过程中，如果网络运营者尚未被《网络关键设备和网络安全专用产品目录（第一批）》所涵盖，是否可以暂时不予履行网络安全认证和检测保护义务。这一问题若处理不当，在未来极有可能演变成网络关键设备和网络安全专用产品提供者或销售者的重大法律风险事件。对于此，我们的观点是只要提供网络关键设备和网络安全专用产品服务，无论是否被《网络关键设备和网络安全专用产品目录（第一批）》所涵盖都应积极履行此义务。

第一，网络关键设备和网络安全专用产品目录的制定其立法目的之一是解决我国认证、检测实践职能交叉、重复认证的问题所采用的立法对策，《网络关键设备和网络安全专用产品目录（第一批）》为判定网络关键设备和网络安全专用产品提供者提供了重要依据，但需要注意的是，在现阶段，该目录不是判定是否承担网络安全认证、检测义务的唯一依据，而是多种判定标准并存。因为，网络关键设备和网络安全专用产品必然属于“强制性产品”。只要是强制性产品，就必然要遵守强制认证的法律要求。因为国家质检总局 117 号令《强制性产品认证管理》第二条明确规定：为保护国家安全、防止欺诈行为、保护人体健康或者安全、保护动植物生命或者健康、保护环境，国家规定的相关产品必须经过认证（以下简称强制性产品认证），并标注认证标志后，方可出厂、销售、进口或者在其他经营活动中使用。

第二，《网络安全法》是网络安全领域的基本法，是国务院或国务院相关职能部门制定的行政法规的上位法，是网络安全法定义务判定的主要依据。为此，网络关键设备和网络安全专用产品的提供者或销售者以下位法暂未做出配套规定为由进行抗辩是无效的。

第三，《网络安全法》对网络安全认证、检测虽然采用促进型立法方式，但对于网络关键设备和网络安全专用产品确是强制性规定，立法用意在于重点预防，从而促进和推动网络安全保障体系构建。对于暂时未被《网络关键设备和网络安全专用产品目录（第一批）》认定的网络关键设备和网络安全专用产品，其当然属于该条的调整对象。为此，只要系网络关键设备和网络安全专用产品提供者，无论是否被《网络关键设备和网络安全专业产品目录（第一批）》所涵盖，都应积极参与。

## （二）“应当”的理解

从法律规范分类视角解读，“应当”属于义务性规范，其旨在为行为主体设定积极的作为义务。这也意味着对于网络关键设备和网络安全专用产品的销售者或提供者来说按照国家有关标准接受认证或检测是必须履行的义务，若不履行，将遭受法律的惩罚。同时，需要注意的是，网络关键设备和网络安全专用产品的销售者或提供者履行这一法定义务，不是以有偿服务为条件的。因为，第二十三

条款文中的“提供”既包括有偿提供，也包括无偿提供。

### （三）在认证或检测委托时需要审查认证或检测机关是否具备相应资质

对网络关键设备或网络安全专用产品进行认证或检测的机构必须具备相应的资质。从网络关键设备或网络安全专用产品提供者或销售者网络安全保护义务遵从的视角出发，在进行认证或检测时，审查认证或检测机关是否具备相应的资质是一个至关重要的问题，否则将直接导致认证或检测无效。关于机构资质的选择，在发布《网络关键设备和网络安全专用产品目录（第一批）》时，提出了明确的界定，“具备资格的机构是指国家认证认可监督管理委员会、工业和信息化部、公安部、国家互联网信息办公室按照国家有关规定共同认定的机构”。对于这一规定，网络关键设备或网络安全专用产品的提供者或销售者需要高度注意，否则极有可能导致认证或检测无效。例如，国家信息安全产品认证唯一指定的机构是中国信息安全认证中心，其认证的范围包括八大类（13 小类），具体为防火墙、网络安全隔离卡与线路选择器、安全隔离与信息交换产品、安全路由器、智能卡、数据备份与恢复产品、安全操作系统、安全数据库系统、反垃圾邮件产品、入侵检测系统（IDS）、网络脆弱性扫描产品、安全审计产品、网站恢复产品。

### （四）认证或检测依据的标准必须是相关国家标准

网络关键设备和网络安全专用产品的认证或检测标准必须是相关的国家标准。关于网络关键设备和网络安全专用产品认证或检测标准，我国已经形成了系列标准。在此时，对于网络关键设备和网络安全专用产品的提供者或销售者必须注意两个方面的问题，一是严格按照我国网络（信息）安全产品对应的国家标准予以认证和检测，二是及时关注相关标准的动态变化可能导致的认证效力转化而引发的法律风险。例如，根据《国家认监委关于部分产品依据新版标准实施国家信息安全产品认证的公告》（国家认监委 2016 年第 15 号公告），国家信息安全产品认证对入侵检测系统（IDS）、网络脆弱性扫描产品、安全审计产品、防火墙、网络安全隔离卡与线路选择器、安全隔离与信息交换产品启用了新版国家标准，即《信息安全技术 网络入侵检测系统技术要求和测试评价方法》（GB/T 20275—2013）、《信息安全技术

网络脆弱性扫描产品安全技术要求》(GB/T 20278—2013)、《信息安全技术 信息系统安全审计产品技术要求和测试评价方法》(GB/T 20945—2013)、《信息安全技术 防火墙安全技术要求和测试评价方法》(GB/T 20281—2015)和《信息安全技术 网络和终端隔离产品安全技术要求》(GB/T 20279—2015)。

### (五) 合理避免重复认证或检测

网络关键设备和网络安全专用产品的缺陷或漏洞可能引发极大的网络安全风险,对其进行强制认证或检测是系网络安全风险预防的考量,但《网络安全法》同时兼顾了安全与发展并重的原则,不能因此阻碍网络关键设备和网络安全专用产品提供者或销售者的发展,这也是我国构建统一认证、检测标准化体系和避免网络安全认证或检测行政机关滥用权力的要求。因为,在我国目前的实践中,有多个政府部门依据各自职责开展网络设备和产品的安全认证和安全检测,产品范围有重复,认证检测的项目有交叉,要求也不统一,致使需要重复认证、检测,造成资源浪费,企业负担加大。为此,制定、公布网络关键设备和网络安全专用产品目录并推动安全认证、安全检测结果互认是《网络安全法》确立的基本对策。随着《网络关键设备和网络安全专用产品目录(第一批)》的制定和公布,我们认为网络关键设备和网络安全专用产品的提供者或销售者可以以此为据拒绝重复认证或检测。

### (六) 提醒认证或检测机构及时报送认证或检测结果

根据国家互联网信息办公室会同工业和信息化部、公安部、国家认证认可监督管理委员会共同发布的《关于发布〈网络关键设备和网络安全专用产品目录(第一批)〉的公告》的规定:网络关键设备、网络安全专用产品选择安全检测方式的,经安全检测符合要求后,由检测机构将网络关键设备、网络安全专用产品检测结果(含本公告发布之前已经本机构安全检测符合要求、且在有效期内的设备与产品)依照相关规定分别报送工业和信息化部、公安部。选择安全认证方式的,经安全认证合格后,由认证机构将认证结果(含本公告发布之前已经本机构安全认证合格、且在有效期内的设备与产品)依照相关规定报送国家认证认可监督管理委员会。从内容看,这虽然是对网络关键设备、网络安全专用产品的认证、检测

机关的及时报送义务提出了要求，但从网络关键设备、网络安全专用产品网络安全保护义务遵从视角来看，我们建议网络关键设备和网络安全专用产品的提供者或销售者应积极提醒认证或检测机构及时报送认证或检测合格的结果，以避免认证、检测机关的过失所引发的法律风险。

### 三、《网络安全法》第二十六条的解读

《网络安全法》第二十六条规定：开展网络安全认证、检测、风险评估等活动，向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息，应当遵守国家有关规定。该条是对开展网络安全服务活动的规定。该条对于规范我国网络安全认证、检测、风险评估、网络安全信息发布等网络安全服务行业具有重大意义，从法律层面为有关部门制定具体办法和开展执法提供了法律依据。

当前，由网络安全认证、检测、风险评估及网络安全信息发布等构成的网络安全服务行业，对于提升我国网络安全产品、服务的质量，建立我国网络安全情报共享体系，构建我国“大安全”风险防控体系等方面起到了不可或缺的重要作用。但是，该行业发展仍然存在着参差不齐、良莠不一的突出问题。例如，有的机构服务不规范，与国家相关法规要求相差甚远，甚至有机构和个人滥用自己的专业技术和掌握的信息，谋取非法利益，这与国家培养和促进该行业的初衷背道而驰。

网络安全认证、检测、风险评估及网络安全信息发布等是网络安全风险主动防御的关键和基础，健全该领域的立法，从法律层面做出总的原则性规定是《网络安全法》的必然选择，也是对前期网络安全认证、检测、风险评估及网络安全信息发布等立法零散化现状的立法总结。

网络安全认证、检测和风险评估制度相关的主要法律法规包括但不限于：《网络安全法》、《认证认可条例》、《国务院办公厅关于加强认证认可工作的通知》、《中华人民共和国产品质量法》（以下简称《产品质量法》）、《中华人民共和国进出口商品检验法》（以下简称《进出口商品检验法》）、《中华人民共和国标准化法》（以下简称《标准化法》）、《中华人民共和国计量法》（以下简称《计量法》）、《中华人民共和国计量法实施细则》（以下简称《计量法实施细则》）、《中华人民共和国标



标准化法实施条例》(以下简称《标准化法实施条例》)、《中华人民共和国进出口商品检验法实施条例》(以下简称《进出口商品检验法实施条例》)、《信息安全等级保护管理办法》、《网络信息安全等级保护制度》、《信息网络传播权保护条例》、《联网单位安全员管理办法》、《公用电信网互联管理规定》、《计算机信息系统安全保护条例》、《电信条例》、《中华人民共和国电子签名法》(以下简称《电子签名法》)、《计算机病毒防治管理办法》、《互联网IP地址管理办法》、《强制性产品认证管理规定》、《强制性产品认证标志管理办法》、《认证咨询机构管理办法》、《认证培训机构管理办法》、《强制性产品认证机构、管理机构和实验室管理办法》、《认证及认证培训、咨询人员管理办法》、《认证证书和认证标志管理办法》、《关于发布〈信息安全管理体系统认证咨询师注册准则〉的通知》、《认证技术规范管理办法》、《强制性产品认证检查员管理办法》、《认证认可申诉、投诉管理办法》、《网络产品和服务安全审查办法(试行)》、《企业内部控制基本规范》、《工业控制系统信息安全防护指南》、《工业控制系统信息安全防护能力评估工作管理办法》、《工业控制系统和信息安全防护能力评估方法》、ISO/IEC27001:2013等。

#### 四、《网络安全法》第三十八条的解读

《网络安全法》第三十八条规定:关键信息基础设施的运营者应当自行或者委托网络安全服务机构对其网络的安全性和可能存在的风险每年至少进行一次检测评估,并将检测评估情况和改进措施报送相关负责关键信息基础设施安全保护工作的部门。该条是关于关键信息基础设施运营者开展网络安全检测评估的规定。

对关键信息基础设施进行法律保护是“互联网+”时代我国的一项战略需求<sup>①</sup>,意义和责任重大,一旦发生严重的信息安全风险事件,将危及整个国家的正常运转。因此,加强关键信息基础设施的安全保护,是《网络安全法》最为重要的内容。如何实现对关键信息基础设施的保护,首要工作在于对关键信息基础设施的风险识别,了解系统自身的脆弱性及可能面临的风险。关键信息基础设施的运营者是安全保护的第一责任人,是对关键信息基础设施可能面临的网络安全风险情

<sup>①</sup> 王玥,马明虎.“互联网+”时代关键基础设施信息安全法律保护研究[J].西北大学学报(哲学社会科学版),2016.

报收集、掌握的最直接者和最便利者，也是最终法律责任承担的最主要责任人，所以，根据信息安全管理要求，《网络安全法》对关键信息基础设施运营者确立网络安全风险检测评估义务及相关要求是应然之义，同时这也是国际惯例。为此，关键信息基础设施的运营者就必须全面、准确、清晰地对该条确立的网络安全保护义务进行界定。我们认为应当重点关注以下关键问题。

### （一）关键信息基础设施的认定

对于什么是“关键信息基础设施”（Critical Information Infrastructure），《网络安全法》并没有给出明确的定义和界定，而是采用了界定性描述。《网络安全法》第三十一条规定：国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。这种界定性描述，虽然可以有效避免概念的争议，增强法律的实施性，但对操作却制造了一定的困境。为此，《信息安全技术，关键信息基础设施网络安全保护要求（草案）》的附录 A，即《关键信息基础设施确定指南》可以为确立关键信息基础设施提供重要的参考。

该指南对关键信息基础设施的界定是指面向公众网络提供网络信息服务或支撑能源、通信、金融、交通、公用事业等重要行业的信息系统或工业控制系统，而且这些系统一旦发生网络安全事故，会严重影响行业正常运行，对国家政治、经济、科技、社会、文化、国防、环境及人民生命财产造成严重损失。此外，并进一步指出可以分为三大类，分别是网站类、平台类和生产业务类，其存在的形态可以是一个信息系统、一个网络、一个工业控制系统，也可以是多个信息系统、网络、工业控制系统的组合。同时，该指南还给出了确立关键信息基础设施的基本步骤：一是确定关键业务，二是确定支撑关键业务的信息系统或工业控制系统，三是根据关键业务或工业控制系统的依赖程度，以及信息系统发生网络安全事件后可能造成的损失认定关键信息基础设施。

### （二）检测评估的主体

《网络安全法》第三十八条所确立的开展关键信息基础设施网络安全风险检测

评估主体既可以是关键信息基础设施运营者自己，也可以是具有网络安全评估资质的第三方。

《网络安全法》第三十八条之所以确立了关键信息基础设施的运营者可以开展自我评估，而没有强制地采用第三方审计监督的模式，主要是考量到关键信息基础设施一旦发生网络安全风险事件所造成后果的严重性，需要贯彻积极防御的风险控制政策。之所以这样做，一是因为对关键信息基础设施的信息安全管理是关键信息基础设施运营者的日常工作；二是因为关键信息基础设施的运营者较之第三方，对关键信息基础设施的日常运行情况、系统风险、数据管理、现有的安全技术措施应对网络威胁的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等掌握得更为全面和直接，一旦出现网络信息安全风险预警，可采用应急方案，能更直接、有效应对；三是因为关键信息基础设施一旦发生重大网络信息安全风险事件所造成后果的严重性，必须对其采用持续改进的原则，贯穿到关键信息基础设施的整个生命周期，即需要根据安全诉求、系统脆弱性、风险威胁程度、系统环境的变化及对系统安全认识的深化等，及时检查、总结，调整现有的安全策略和保护措施，持续改进网络安全管理体系的有效性。因此，关键信息基础设施运营者自我开展网络安全风险检测、评估是必然并且是预防关键信息基础设施网络安全风险的主要力量。

根据《网络安全法》第三十八条的规定，关键信息基础设施的运营者对于《网络安全法》确立的强制性网络安全风险评估制度，可以委托第三方完成。此时，从关键信息基础设施运营者法律遵从的视角来看，委托的第三方必须具备相应的资质和能力，否则将不能有效应对其可能面临的网络安全风险。在我国，开展网络安全风险检测评估，采用了严格的认证认可制度。根据中国信息安全认证中心官网显示，截至2017年8月30号，我国具有网络安全风险评估的机构（包括一级资质、二级资质、三级资质）共计225家。

### （三）检测评估的依据及评估方法的选择

网络安全风险评估依据的选择是开展网络安全风险评估的关键。但《网络安全法》第三十八条却未对关键信息基础设施的运营者网络安全风险评估规定具体的指示性规范。对此，我们认为《网络安全法》第三十八条的立法目的旨在从网络信息

安全管理、内部风险控制实现的视角对关键信息基础设施运营者界定网络安全保护义务，因此，网络运营者的网络信息安全管理遵从规范应当是自我检测评估或第三方机构开展检测评估的依据（或标准）。2017年8月1日，由中国信息安全认证中心发布的《信息安全服务规范》附录A——信息安全风险评估服务资质专业评价要求的具体规定也印证了这一判断。我们认为，2014年美国国家技术研究院制定的《提升关键基础设施网络安全框架》、我国2009年开始实施的《企业内部控制基本规范》、信息安全领域认可度极高的ISO27001体系、2016年工信部发布的《工业控制系统信息安全防护指南》、《工业控制系统信息安全防护能力评估工作管理办法》（内附《工业控制系统信息安全防护能力评估方法》）等可以作为检测评估依据方法的参照。

#### （四）其他注意事项

第一，对于关键信息基础设施运营者开展网络安全风险评估这一网络安全保护义务，其性质属于强制性义务。因为，《网络安全法》第三十八条明确规定为“应当”。

第二，每年至少进行一次网络安全风险评估。《网络安全法》第三十八条之所以规定为每年至少进行一次，而不具体规定次数，一是出于对关键信息基础设施网络安全保护的特性，需要采用持续改进的原则；二是出于对关键信息基础设施运营者法律遵从成本的考量。

第三，关键信息基础措施的运营者还应当将检测评估情况和改进措施及时报送，接受相关部门的指导和监督。这里需要注意的是网络安全风险检测评估情况和改进措施报告应当满足报送要求。由于《网络安全法》没有对此做出具体的要求和规定，但基于实效安全观及对关键信息基础设施实现网络安全风险的有效预防，只要以实质性符合为目标做出的评估报告和改进措施都应当属于报告的内容。

### 五、其他相关部分条款的解读

《网络安全法》第三十九条规定，国家网信部门应当统筹协调有关部门对关键信息基础设施的安全保护采取下列措施：对关键信息基础设施的安全风险进行抽

查检测，提出改进措施，必要时可以委托网络安全服务机构对网络存在的安全风险进行检测评估。该条所规定的有关网络安全风险检测评估，是在《网络安全法》第三十八条基础之上，对国家网信部门针对关键基础设施保护提出的要求。第三十九条是对第三十八条的进一步补充，从网络运营者的法律遵从视角来看，需要注意问题包括两个方面，一是对网信部门提出的改进措施予以接受；二是配合国家网络信息部门的抽查检测，以及国家网信部门委托的网络安全服务机构开展的网络安全风险评估工作。

除此之外，在《网络安全法》其他条文中，也涉及网络安全检测、认证和风险评估相关规定。但基本要求都是积极协助、接受主管部门指导和监督。

## 第二节 网络安全认证、检测及风险评估制度概述

网络安全认证、检测及风险评估制度是科学分析并确定风险的过程，是网络信息安全建设的起点，是需求主导和突出重点原则的具体体现，是组织机构实现信息系统安全的重要步骤，是网络安全风险管理的基本前提和基础。

但该制度的确立和发展不是一蹴而就的，它以网络安全认知为根据逐步深化。以最早关注网络信息安全和网络安全评估的美国为例，也经历了三个阶段，从最初只关心计算机保密逐渐发展到以计算机和网络为对象，最后到对网络信息系统的设施对象。目前美国已经建立了国家安全评估体系，负责研究并开发了系列的评估标准、评估技术和评估认证方法。我国对网络安全评估也经历了一个逐渐深化的过程，早期安全工作的重点是信息保密，20世纪80年代后，提出了计算机安全问题，并开展了计算机安全检查工作，但由于对于风险的认识不足，并常采用一些绝对安全措施，到了20世纪90年代，我国提出了计算机信息系统安全等级保护的要求，并逐步提出了一系列的相关技术标准与管理规范，网络安全的风险意识开始形成并逐渐加强，现正在逐步尝试建立网络安全标准体系。

时至今日，网络信息安全的发展经历通信保密、计算机安全、IT安全、信

息安全保障四个阶段。当下，是以保障信息化带来的最大化利益为宗旨，以信息和信息系统为对象，以技术、管理、法律为保障能力来源，在局域计算环境、边界和外部连接、基础设施、信息内容四个层面，根据信息产生、存储、处理、传输、消亡五个状态，以及预警（W）、保护（P）、检测（D）、响应（R）、恢复（R）、反击（C）六个保障环节来构建信息安全风险防控保障体系，最终实现保密性、完整性、可用性、可认证性、不可否认性、可控性、可追究性七个信息安全属性是人们应对网络信息安全的策略选择。简言之，以信息安全风险管理应对信息安全问题是当下的策略，其中网络安全认证、检测及风险评估制度是关键和基础。

当下对网络安全认证、检测及风险评估的认识主要是从网络（信息安全）风险管理的视角予以认知。其中，网络安全认证，根据《中华人民共和国认证认可条例》的规定，是指由认证机构证明产品、服务、管理体系符合相关技术规范、相关技术规范的强制性要求或者标准的合格评定活动；网络安全风险评估根据中国信息安全认证中心发布的《信息安全服务规范》的界定来看，是指对特定威胁利用单个或一组资产脆弱性的可能性及由此可能给组织带来的损害进行识别、分析和评价的过程。

### 第三节 网络安全认证、检测及风险评估 法规遵从框架及建议

网络（信息）安全风险管理是当下应对网络（信息）安全风险、实现网络（信息）保障的共识。网络安全认证、检测及风险评估是网络（信息）安全风险管理的关键和基础，网络运营者是网络安全风险管理的重要协同主体。网络安全法治对此的保障，首要在于网络运营者对法律法规的遵从，关键在于最低保障义务的确立。但《网络安全法》立法却未对网络安全认证、检测及风险评估的具体内容做出具体指引和示范性规定，因此，本章以《网络安全法》为整体要求，以前期相关配套政策、标准等为主要内容，以实现实质性符合为目标，梳理了网络运营

者的网络安全认证、检测及风险评估法规遵从框架，并以风险有效识别和主动预防为指引，提出了相关遵从框架和建议。

一、网络安全认证、检测及风险评估法规遵从框架

网络安全认证、检测及风险评估法规遵从框架如表 8-1 所示。

表 8-1 网络安全认证、检测及风险评估法规遵从框架

法律名称	法律条款	法律规定
《产品质量法》	第三条	生产者、销售者应当建立健全内部产品质量管理制度，严格实施岗位质量规范、质量责任以及相应的考核办法
	第五条	禁止伪造或者冒用认证标志等质量标志；禁止伪造产品的产地，伪造或者冒用他人的厂名、厂址；禁止在生产、销售的产品中掺杂、掺假，以假充真，以次充好
	第十三条	可能危及人体健康和人身、财产安全的工业产品，必须符合保障人体健康和人身、财产安全的国家标准、行业标准；未制定国家标准、行业标准的，必须符合保障人体健康和人身、财产安全的要求。禁止生产、销售不符合保障人体健康和人身、财产安全的标准和要求的工业产品。具体管理办法由国务院规定
	第十六条	对依法进行的产品质量监督检查，生产者、销售者不得拒绝
	第十七条	依照本法规定进行监督抽查的产品质量不合格的，由实施监督抽查的产品质量监督部门责令其生产者、销售者限期改正。逾期不改正的，由省级以上人民政府产品质量监督部门予以公告；公告后经复查仍不合格的，责令停业，限期整顿；整顿期满后经复查产品质量仍不合格的，吊销营业执照。监督抽查的产品有严重质量问题的，依照本法第五章的有关规定处罚
	第十九条	产品质量检验机构必须具备相应的检测条件和能力，经省级以上人民政府产品质量监督部门或者其授权的部门考核合格后，方可承担产品质量检验工作。法律、行政法规对产品质量检验机构另有规定的，依照有关法律、行政法规的规定执行
	第二十条	从事产品质量检验、认证的社会中介机构必须依法设立，不得与行政机关和其他国家机关存在隶属关系或者其他利益关系
	第二十一条	产品质量检验机构、认证机构必须依法按照有关标准，客观、公正地出具检验结果或者认证证明。产品质量认证机构应当依照国家规定对准许使用认证标志的产品进行认证后的跟踪检查；对不符合认证标准而使用认证标志的，要求其改正；情节严重的，取消其使用认证标志的资格

续表

法律名称	法律条款	法律规定
《产品质量法》	第二十六条	生产者应当对其生产的产品质量负责。产品质量应当符合下列要求：（一）不存在危及人身、财产安全的不合理的危险，有保障人体健康和人身、财产安全的国家标准、行业标准的，应当符合该标准；（二）具备产品应当具备的使用性能，但是，对产品存在使用性能的瑕疵做出说明的除外；（三）符合在产品或者其包装上注明采用的产品标准，符合以产品说明、实物样品等方式表明的质量状况
	第二十七条	产品或者其包装上的标识必须真实，并符合下列要求：（一）有产品质量检验合格证明；（二）有中文标明的产品名称、生产厂厂名和厂址；（三）根据产品的特点和使用要求，需要标明产品规格、等级、所含主要成分的名称和含量的，用中文相应予以标明；需要事先让消费者知晓的，应当在外包装上标明，或者预先向消费者提供有关资料；（四）限期使用的产品，应当在显著位置清晰地标明生产日期和安全使用期或者失效日期；（五）使用不当，容易造成产品本身损坏或者可能危及人身、财产安全的产品，应当有警示标志或者中文警示说明。裸装的食品和其他根据产品的特点难以附加标识的裸装产品，可以不附加产品标识
	第二十八条	易碎、易燃、易爆、有毒、有腐蚀性、有放射性等危险物品以及储运中不能倒置和其他有特殊要求的产品，其包装质量必须符合相应要求，依照国家有关规定做出警示标志或者中文警示说明，标明储运注意事项
	第二十九条	生产者不得生产国家明令淘汰的产品
	第三十条	生产者不得伪造产地，不得伪造或者冒用他人的厂名、厂址
	第三十一条	生产者不得伪造或者冒用认证标志等质量标志
	第三十二条	生产者生产产品，不得掺杂、掺假，不得以假充真、以次充好，不得以不合格产品冒充合格产品
	第三十三条	销售者应当建立并执行进货检查验收制度，验明产品合格证明和其他标识
	第三十四条	销售者应当采取措施，保持销售产品的质量
	第三十五条	销售者不得销售国家明令淘汰并停止销售的产品和失效、变质的产品
	第三十六条	销售者销售的产品的标识应当符合本法第二十七条的规定
	第三十七条	销售者不得伪造产地，不得伪造或者冒用他人的厂名、厂址
	第三十八条	销售者不得伪造或者冒用认证标志等质量标志
	第三十九条	销售者销售产品，不得掺杂、掺假，不得以假充真、以次充好，不得以不合格产品冒充合格产品



续表

法律名称	法律条款	法律规定
《产品质量法》	第四十条	售出的产品有下列情形之一的，销售者应当负责修理、更换、退货；给购买产品的消费者造成损失的，销售者应当赔偿损失：（一）不具备产品应当具备的使用性能而事先未作说明的；（二）不符合在产品或者其包装上注明采用的产品标准的；（三）不符合以产品说明、实物样品等方式表明的质量状况的。销售者依照前款规定负责修理、更换、退货、赔偿损失后，属于生产者的责任或者属于向销售者提供产品的其他销售者（以下简称供货者）的责任的，销售者有权向生产者、供货者追偿。销售者未按照第一款规定给予修理、更换、退货或者赔偿损失的，由产品质量监督部门或者工商行政管理部门责令改正。生产者之间，销售者之间，生产者与销售者之间订立的买卖合同、承揽合同有不同约定的，合同当事人按照合同约定执行
	第四十一条	因产品存在缺陷造成人身、缺陷产品以外的其他财产（以下简称他人财产）损害的，生产者应当承担赔偿责任。生产者能够证明有下列情形之一的，不承担赔偿责任：（一）未将产品投入流通的；（二）产品投入流通时，引起损害的缺陷尚不存在的；（三）将产品投入流通时的科学技术水平尚不能发现缺陷的存在的
	第四十二条	由于销售者的过错使产品存在缺陷，造成人身、他人财产损害的，销售者应当承担赔偿责任。销售者不能指明缺陷产品的生产者也不能指明缺陷产品的供货者的，销售者应当承担赔偿责任
	第四十三条	因产品存在缺陷造成人身、他人财产损害的，受害人可以向产品的生产者要求赔偿，也可以向产品的销售者要求赔偿。属于产品的生产者的责任，产品的销售者赔偿的，产品的销售者有权向产品的生产者追偿。属于产品的销售者的责任，产品的生产者赔偿的，产品的生产者有权向产品的销售者追偿
	第四十四条	因产品存在缺陷造成受害人人身伤害的，侵害人应当赔偿医疗费、治疗期间的护理费、因误工减少的收入等费用；造成残疾的，还应当支付残疾人生活自助具费、生活补助费、残疾赔偿金以及由其扶养的人所必需的生活费等费用；造成受害人死亡的，并应当支付丧葬费、死亡赔偿金以及由死者生前扶养的人所必需的生活费等费用。因产品存在缺陷造成受害人财产损失的，侵害人应当恢复原状或者折价赔偿。受害人因此遭受其他重大损失的，侵害人应当赔偿损失
《进出口商品检验法》	第四条	进出口商品检验应当根据保护人类健康和国家安全、保护动物或者植物的生命和健康、保护环境、防止欺诈行为、维护国家安全的原则，由国家商检部门制定、调整必须实施检验的进出口商品目录（以下简称目录）并公布实施

续表

法律名称	法律条款	法律规定
《进出口商品检验法》	第五条	列入目录的进出口商品，由商检机构实施检验。前款规定的进口商品未经检验的，不准销售、使用；前款规定的出口商品未经检验合格的，不准出口。本条第一款规定的进出口商品，其中符合国家规定的免于检验条件的，由收货人或者发货人申请，经国家商检部门审查批准，可以免于检验
	第六条	必须实施的进出口商品检验，是指确定列入目录的进出口商品是否符合国家技术规范的强制性要求的合格评定活动。合格评定程序包括：抽样、检验和检查；评估、验证和合格保证；注册、认可和批准以及各项的组合
	第七条	列入目录的进出口商品，按照国家技术规范的强制性要求进行检验；尚未制定国家技术规范的强制性要求的，应当依法及时制定，未制定之前，可以参照国家商检部门指定的国外有关标准进行检验。第十一条本法规定必须经商检机构检验的进口商品的收货人或者其代理人，应当向报关地的商检机构报检。海关凭商检机构签发的货物通关证明验放
	第十二条	本法规定必须经商检机构检验的进口商品的收货人或者其代理人，应当在商检机构规定的地点和期限内，接受商检机构对进口商品的检验。商检机构应当在国家商检部门统一规定的期限内检验完毕，并出具检验证单
	第十三条	本法规定必须经商检机构检验的进口商品以外的进口商品的收货人，发现进口商品质量不合格或者残损短缺，需要由商检机构出证索赔的，应当向商检机构申请检验出证
	第十四条	对重要的进口商品和大型的成套设备，收货人应当依据对外贸易合同约定在出口国装运前进行预检验、监造或者监装，主管部门应当加强监督；商检机构根据需要可以派出检验人员参加
	第十五条	本法规定必须经商检机构检验的出口商品的发货人或者其代理人，应当在商检机构规定的地点和期限内，向商检机构报检。商检机构应当在国家商检部门统一规定的期限内检验完毕，并出具检验证单。对本法规定必须实施检验的出口商品，海关凭商检机构签发的货物通关证明验放
	第十六条	经商检机构检验合格发给检验证单的出口商品，应当在商检机构规定的期限内报关出口；超过期限的，应当重新报检
	第十七条	为出口危险货物生产包装容器的企业，必须申请商检机构进行包装容器的性能鉴定。生产出口危险货物的企业，必须申请商检机构进行包装容器的使用鉴定。使用未经鉴定合格的包装容器的危险货物，不准出口

续表

法律名称	法律条款	法律规定
《标准化法》	第十四条	强制性标准，必须执行。不符合强制性标准的产品，禁止生产、销售和进口。推荐性标准，国家鼓励企业自愿采用
	第十五条	企业对有国家标准或者行业标准的产品，可以向国务院标准化行政主管部门或者国务院标准化行政主管部门授权的部门申请产品质量认证。认证合格的，由认证部门授予认证证书，准许在产品或者其包装上使用规定的认证标志。已经取得认证证书的产品不符合国家标准或者行业标准的，以及产品未经认证或者认证不合格的，不得使用认证标志出厂销售
《中华人民共和国计量法》（以下简称《计量法》）	第十二条	制造、修理计量器具的企业、事业单位，必须具备与所制造、修理的计量器具相适应的设施、人员和检定仪器设备，经县级以上人民政府计量行政部门考核合格，取得《制造计量器具许可证》或者《修理计量器具许可证》。制造、修理计量器具的企业未取得《制造计量器具许可证》或者《修理计量器具许可证》的，工商行政管理部门不予办理营业执照
	第十三条	制造计量器具的企业、事业单位生产本单位未生产过的计量器具新产品，必须经省级以上人民政府计量行政部门对其样品的计量性能考核合格，方可投入生产
	第十四条	未经国务院计量行政部门批准，不得制造、销售和进口国务院规定废除的非法定计量单位的计量器具和国务院禁止使用的其他计量器具
	第十五条	制造、修理计量器具的企业、事业单位必须对制造、修理的计量器具进行检定，保证产品计量性能合格，并对合格产品出具产品合格证。县级以上人民政府计量行政部门应当对制造、修理的计量器具的质量进行监督检查
	第十六条	进口的计量器具，必须经省级以上人民政府计量行政部门检定合格后，方可销售
	第十七条	使用计量器具不得破坏其准确度，损害国家和消费者的利益
	第十八条	个体工商户可以制造、修理简易的计量器具。制造、修理计量器具的个体工商户，必须经县级人民政府计量行政部门考核合格，发给《制造计量器具许可证》或者《修理计量器具许可证》后，方可向工商行政管理部门申请营业执照。个体工商户制造、修理计量器具的范围和管理办法，由国务院计量行政部门制定
	第二十二条	为社会提供公证数据的产品质量检验机构，必须经省级以上人民政府计量行政部门对其计量检定、测试的能力并可靠性考核合格
《认证认可条例》	第二十五条	获得认证证书的，应当在认证范围内使用认证证书和认证标志，不得利用产品、服务认证证书、认证标志和相关文字、符号，误导公众认为其管理体系已通过认证，也不得利用管理体系认证证书、认证标志和相关文字、符号，误导公众认为其产品、服务已通过认证

续表

法律名称	法律条款	法律规定
《认证认可条例》	第二十八条	为了保护国家安全、防止欺诈行为、保护人体健康或者安全、保护动植物生命或者健康、保护环境，国家规定相关产品必须经过认证的，应当经过认证并标注认证标志后，方可出厂、销售、进口或者在其他经营活动中使用
	第三十条	列入目录的产品，必须经国务院认证认可监督管理部门指定的认证机构进行认证。列入目录产品的认证标志，由国务院认证认可监督管理部门统一规定
	第四十七条	取得认可的机构应当在取得认可的范围内使用认可证书和认可标志。取得认可的机构不当使用认可证书和认可标志的，认可机构应当暂停其使用直至撤销认可证书，并予公布
《进出口商品检验法实施条例》	第十六条	法定检验的进口商品的收货人应当持合同、发票、装箱单、提单等必要的凭证和相关批准文件，向海关报关地的出入境检验检疫机构报检；海关放行后 20 日内，收货人应当依照本条例第十八条的规定，向出入境检验检疫机构申请检验。法定检验的进口商品未经检验的，不准销售，不准使用。进口实行验证管理的商品，收货人应当向海关报关地的出入境检验检疫机构申请验证。出入境检验检疫机构按照国家质检总局的规定实施验证
	第二十四条	法定检验的出口商品的发货人应当根据国家质检总局统一规定的地点和期限内，持合同等必要的凭证和相关批准文件向出入境检验检疫机构报检。法定检验的出口商品未经检验或者经检验不合格的，不准出口。出口商品应当在商品的生产地检验。国家质检总局可以根据便利对外贸易和进出口商品检验工作的需要，指定在其他地点检验。出口实行验证管理的商品，发货人应当向出入境检验检疫机构申请验证。出入境检验检疫机构按照国家质检总局的规定实施验证
《标准化法实施条例》	第十七条	企业生产的产品没有国家标准、行业标准和地方标准的，应当制定相应的企业标准，作为组织生产的依据。企业标准由企业组织制定（农业企业标准制定办法另定），并按省、自治区、直辖市人民政府的规定备案。对已有国家标准、行业标准或者地方标准的，鼓励企业制定严于国家标准、行业标准或者地方标准要求的企 业标准，在企业内部适用
	第二十三条	从事科研、生产、经营的单位和个人，必须严格执行强制性标准。不符合强制性标准的产品，禁止生产、销售和进口
	第二十四条	企业生产执行国家标准、行业标准、地方标准或企业标准，应当在产品或其说明书、包装物上标注所执行标准的代号、编号、名称
	第二十五条	出口产品的技术要求由合同双方约定。出口产品在国内销售时，属于我国强制性标准管理范围的，必须符合强制性标准的要求
	第二十六条	企业研制新产品、改进产品、进行技术改造，应当符合标准化要求

续表

法律名称	法律条款	法律规定
《强制性产品认证管理规定》	第八条	强制性产品认证应当适用以下单一认证模式或者多项认证模式的组合，具体模式包括：（一）设计鉴定；（二）型式试验；（三）生产现场抽取样品检测或者检查；（四）市场抽样检测或者检查；（五）企业质量保证能力和产品一致性检查；（六）获证后的跟踪检查。产品认证模式应当依据产品的性能，对涉及公共安全、人体健康和环境等方面可能产生的危害程度、产品的生命周期、生产、进口产品的风险状况等综合因素，按照科学、便利等原则予以确定
	第十条	认证委托人应当按照具体产品认证规则的规定，向认证机构提供相关技术材料。销售者、进口商作为认证委托人时，还应当向认证机构提供销售者与生产者或者进口商与生产者订立的相关合同副本。委托其他企业生产列入目录产品的，认证委托人还应当向认证机构提供委托企业与被委托企业订立的相关合同副本
	第十一条	列入目录产品的生产者或者销售者、进口商（以下统称认证委托人）应当委托经国家认监委指定的认证机构（以下简称认证机构）对其生产、销售或者进口的产品进行认证。委托其他企业生产列入目录产品的，委托企业或者被委托企业均可以向认证机构进行认证委托
	第十三条	认证委托人应当保证其提供的样品与实际生产的产品一致，认证机构应当对认证委托人提供样品的真实性进行审查
	第二十三条	获证产品及其销售包装上标注认证证书所含内容的，应当与认证证书的内容相一致，并符合国家有关产品标识标注管理规定
	第二十四条	有下列情形之一的，认证委托人应当向认证机构申请认证证书的变更，由认证机构根据不同情况做出相应处理：（一）获证产品命名方式改变导致产品名称、型号变化或者获证产品的生产者、生产企业名称、地址名称发生变更的，经认证机构核实后，变更认证证书；（二）获证产品型号变更，但不涉及安全性能和电磁兼容内部结构变化；或者获证产品减少同种产品型号的，经认证机构确认后，变更认证证书；（三）获证产品的关键元器件、规格和型号，以及涉及整机安全或者电磁兼容的设计、结构、工艺和材料或者原材料生产企业等发生变更的，经认证机构重新检测合格后，变更认证证书；（四）获证产品生产企业地点或者其质量保证体系、生产条件等发生变更的，经认证机构重新工厂检查合格后，变更认证证书；（五）其他应当变更的情形
	第二十五条	认证委托人需要扩展其获证产品覆盖范围的，应当向认证机构申请认证证书的扩展，认证机构应当核查扩展产品与原获证产品的一致性，确认原认证结果对扩展产品的有效性。经确认合格后，可以根据认证委托人的要求单独出具认证证书或者重新出具认证证书

续表

法律名称	法律条款	法律规定
《强制性产品认证标志管理办法》	第十一条	获得认证的产品使用认证标志的方式可以根据产品特点按以下规定选取：（一）统一印制标准规格认证标志，必须加施在获得认证产品外体规定的位置上；（二）印刷、模压认证标志的，该认证标志应当被印刷、模压在铭牌或产品外体的明显位置上；（三）在相关获得认证产品的本体上不能加施认证标志的，其认证标志必须加施在产品的最小包装上及随附文件中；（四）获得认证的特殊产品不能按以上各款规定加施认证标志的，必须在产品本体上印刷或者模压“中国强制认证”标志的特殊式样
	第十二条	获得认证的产品可以在产品外包装上加施认证标志
	第十三条	在境外生产、并获得认证的产品必须在进口前加施认证标志；在境内生产、并获得认证的产品必须在出厂前加施认证标志
	第十六条	认证标志的申请使用（一）申请人必须持申请书和认证证书的副本向指定的机构申请使用认证标志；（二）申请人委托他人申请使用认证标志的，受托人必须持申请人的委托书、申请书和认证证书的副本向指定的机构申请使用认证标志；（三）申请人以函件或者电讯方式申请使用认证标志的，必须向指定的机构提供申请书、认证证书副本的书面或者电子文本，申请使用认证标志
	第十七条	申请人申请使用认证标志，应当按照国家规定缴纳统一印制标准规格认证标志的工本费或者模压、印刷认证标志的监督管理费
	第二十一条	申请人应当遵守以下规定：（一）建立认证标志的使用和管理制度，对认证标志的使用情况如实记录和存档；（二）保证使用认证标志的产品符合认证要求；（三）对超过认证有效期的产品，不得使用认证标志；（四）在广告、产品介绍等宣传材料中正确地使用认证标志，不得利用认证标志误导、欺诈消费者；（五）接受国家认证认可监督管理委员会、各地质检行政部门和指定认证机构对认证标志使用情况的监督检查
《电信条例》	第七条	国家对电信业务经营按照电信业务分类，实行许可制度。经营电信业务，必须依照本条例的规定取得国务院信息产业主管部门或者省、自治区、直辖市电信管理机构颁发的电信业务经营许可证。如未取得电信业务经营许可证，任何组织或者个人不得从事电信业务经营活动
	第八条	经营基础电信业务，须经国务院信息产业主管部门审查批准，取得《基础电信业务经营许可证》。经营增值电信业务，业务覆盖范围在两个以上省、自治区、直辖市的，须经国务院信息产业主管部门审查批准，取得《跨地区增值电信业务经营许可证》；业务覆盖范围在一个省、自治区、直辖市行政区域内的，须经省、自治区、直辖市电信管理机构审查批准，取得《增值电信业务经营许可证》。运用新技术试办《电信业务分类目录》未列出的新型电信业务的，应当向省、自治区、直辖市电信管理机构备案

续表

法律名称	法律条款	法律规定
《电信条例》	第十四条	申请经营增值电信业务，应当根据本条例第九条第二款的规定，向国务院信息产业主管部门或者省、自治区、直辖市电信管理机构提出申请，并提交本条例第十三条规定的相关文件。申请经营的增值电信业务，按照国家有关规定须经有关主管部门审批的，还应当提交有关主管部门审核同意的文件。国务院信息产业主管部门或者省、自治区、直辖市电信管理机构应当自收到申请之日起 60 日内审查完毕，做出批准或者不予批准的决定。予以批准的，颁发《跨地区增值电信业务经营许可证》或者《增值电信业务经营许可证》；不予批准的，应当书面通知申请人并说明理由
	第十五条	电信业务经营者在经营过程中，变更经营主体、业务范围或者停止经营的，应当提前 90 日向原颁发许可证的机关提出申请，并办理相应手续；停止经营的，还应当按照国家有关规定做好善后工作
	第十六条	经批准经营电信业务的，应当持依法取得的电信业务经营许可证，向企业登记机关办理登记手续
《互联网信息服务管理办法》	第四条	国家对经营性互联网信息服务实行许可制度；对非经营性互联网信息服务实行备案制度。未取得许可或者未履行备案手续的，不得从事互联网信息服务
	第五条	从事新闻、出版、教育、医疗保健、药品和医疗器械等互联网信息服务，依照法律、行政法规以及国家有关规定须经有关主管部门审核同意的，在申请经营许可或者履行备案手续前，应当依法经有关主管部门审核
	第六条	从事经营性互联网信息服务，除应当符合《电信条例》规定的要求外，还应当具备下列条件：（一）有业务发展计划及相关技术方案；（二）有健全的网络与信息安全保障措施，包括网站安全保障措施、信息安全保密管理制度、用户信息安全管理制度；（三）服务项目属于本办法第五条规定范围的，已取得有关主管部门同意的文件
《中华人民共和国电子签名法》（以下简称《电子签名法》）	第十六条	电子签名需要第三方认证的，由依法设立的电子认证服务提供者提供认证服务
	第十七条	提供电子认证服务，应当具备下列条件：（一）具有与提供电子认证服务相适应的专业技术人员和管理人员；（二）具有与提供电子认证服务相适应的资金和经营场所；（三）具有符合国家安全标准的技术和设备；（四）具有国家密码管理机构同意使用密码的证明文件；（五）法律、行政法规规定的其他条件

续表

法律名称	法律条款	法律规定
《中华人民共和国 电子签名法》（以下 简称《电子签名法》）	第十八条	从事电子认证服务，应当向国务院信息产业主管部门提出申请，并提交符合本法第十七条规定条件的相关材料。国务院信息产业主管部门接到申请后经依法审查，征求国务院商务主管部门等有关部门的意见后，自接到申请之日起 45 日内做出许可或者不予许可的决定。予以许可的，颁发电子认证许可证书；不予许可的，应当书面通知申请人并告知理由。申请人应当持电子认证许可证书依法向工商行政管理部门办理企业登记手续。取得认证资格的电子认证服务提供者，应当按照国务院信息产业主管部门的规定在互联网上公布其名称、许可证号等信息
	第十九条	电子认证服务提供者应当制定、公布符合国家有关规定的电子认证业务规则，并向国务院信息产业主管部门备案。电子认证业务规则应当包括责任范围、作业操作规范、信息安全保障措施等事项
	第二十条	电子签名人向电子认证服务提供者申请电子签名认证证书，应当提供真实、完整和准确的信息。电子认证服务提供者收到电子签名认证证书申请后，应当对申请人的身份进行查验，并对有关材料进行审查
	第二十一条	电子认证服务提供者签发的电子签名认证证书应当准确无误，并应当载明下列内容：（一）电子认证服务提供者名称；（二）证书持有人名称；（三）证书序列号；（四）证书有效期；（五）证书持有人的电子签名验证数据；（六）电子认证服务提供者的电子签名；（七）国务院信息产业主管部门规定的其他内容
	第二十二条	电子认证服务提供者应当保证电子签名认证证书内容在有效期内完整、准确，并保证电子签名依赖方能够证实或者了解电子签名认证证书所载内容及其他有关事项
	第二十三条	电子认证服务提供者拟暂停或者终止电子认证服务的，应当在暂停或者终止服务 90 日前，就业务承接及其他有关事项通知有关各方。电子认证服务提供者拟暂停或者终止电子认证服务的，应当在暂停或者终止服务 60 日前向国务院信息产业主管部门报告，并与其他电子认证服务提供者就业务承接进行协商，做出妥善安排。电子认证服务提供者未能就业务承接事项与其他电子认证服务提供者达成协议的，应当申请国务院信息产业主管部门安排其他电子认证服务提供者承接其业务。电子认证服务提供者被依法吊销电子认证许可证书的，其业务承接事项的处理按照国务院信息产业主管部门的规定执行
	第二十四条	电子认证服务提供者应当妥善保存与认证相关的信息，信息保存期限至少为电子签名认证证书失效后 5 年
《计算机病毒防治 管理办法》	第十三条	任何单位和个人销售、附赠的计算机病毒防治产品，应当具有计算机信息系统安全专用产品销售许可证，并贴有“销售许可”标记



续表

法律名称	法律条款	法律规定
《计算机病毒防治管理办法》	第十四条	从事计算机设备或者媒体生产、销售、出租、维修行业的单位和个人，应当对计算机设备或者媒体进行计算机病毒检测、清除工作，并备有检测、清除的记录
	第十五条	任何单位和个人应当接受公安机关对计算机病毒防治工作的监督、检查和指导
《信息安全保护管理办法》	第十条	信息系统建设完成后，其运营、使用单位应当依据本办法选择具有国家相关技术资质和安全资质的测评单位，按照技术标准进行安全测评，符合要求的，方可投入使用

二、安全认证、检测及风险评估法规遵从建议

网络信息安全风险管理是当下应对网络安全风险的策略。网络安全认证、检测是网络信息安全风险识别早期的关键和基础工作，动态化网络安全风险评估是网络信息安全风险管理实现的保障。基于此，主要从网络信息安全管理对一般网络运营者的法规遵从提出了相应建议（见表 8-2）。

表 8-2 网络安全认证、检测及风险评估法规遵从建议

控制项	网络安全认证、检测及风险评估法规遵从建议	对应条款
网络安全认证、检测		《网络安全法》第十七条规定：国家推进网络安全社会化服务体系建设，鼓励有关企业、机构开展网络安全认证、检测和风险评估等安全服务。
是否需要必须经过强制性认证、检测义务的判定	一般而言，从事信息安全服务的网络运营者均需要通过认证或检测（例如，风险评估服务、安全集成服务、应急处理服务、灾难备份与恢复服务、软件安全开发服务、安全运营）。  《网络关键设备和网络安全专用产品目录（第一批）》界定的必须接受强制性认证、检测	《网络安全法》第二十三条规定：网络关键设备和网络安全专用产品应当按照相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求后，方可销售或者提供。国家网信部门会同国务院有关部门制定、公布网络关键
网络安全服务提供者的通用评价要求	法律地位要求  在中华人民共和国境内注册的独立法人组织，发展历程清晰，产权关系明确；  遵循国家相关法律法规、标准要求，无违法违规记录，资信状况良好。  财务资信要求  近 3 年经营状况良好，财务数据真实可信，能够提供本单位出具的近 3 年财务报表（加盖单位公章）。  办公场所要求	

续表

控制项	网络安全认证、检测及风险评估法规遵从建议	对应条款
网络安全服务提供者的通用评价要求	<p>拥有长期办公场所，能够满足机构设置及其业务需要。</p> <p>人员能力要求</p> <p>业绩要求</p> <p>从事信息安全服务（与申报类别一致）4 个月以上；近 3 年内签订完成至少一个信息安全服务（与申报类别一致）项目。</p> <p>服务管理要求</p> <p>建立与运行人员管理程序，明确能力考核指标并制定业务和技能培训计划，定期对相关人员开展培训与考核；</p> <p>建立文档控制程序，明确文档管理职责，任命管理人员，并按照制度执行；</p> <p>建立项目管理制度，明确项目管理职责，任命管理人员，并按照制度执行风险管理；</p> <p>建立并运行保密管理制度，明确岗位保密责任。能够定期对相关人员进行保密教育，并签订保密协议；</p> <p>建立供应商管理制度，确保供应商能够满足服务安全要求（仅适用于安全集成、安全运营、灾难备份与恢复方向）；</p> <p>建立合同管理制度，制定统一合同模板，按照合同约定实施信息安全服务项目。按照客户要求，对于接触的客户敏感信息和知识产权信息予以保护，并确保服务方人员了解客户的相关要求。</p> <p>服务技术要求</p> <p>建立信息安全服务流程，并按照流程实施；</p> <p>建立信息安全服务规范，并按照规范实施</p>	<p>设备和网络安全专用产品目录，并推动安全认证和安全检测结果互认，避免重复认证、检测。</p> <p>《网络安全法》第三十八条规定：关键信息基础设施的运营者应当自行或者委托网络安全服务机构对其网络的安全性和可能存在的风险每年至少进行一次检测评估，并将检测评估情况和改进措施报送相关负责关键信息基础设施安全保护工作的部门</p>
风险评估（依据 PDCA 四个环节展开）		
计划（Plan）	<p>建立信息安全管理 体系（Information Security Management, ISMS）体系，包括它的范围、方针、风险评估和管理、管理者授权实施和运行 ISMS、适用性声明等。</p> <p>ISMS 的范围：根据业务、组织、位置、资产和技术等方面的特性，确定 ISMS 的范围和边界，包括对范围的任何删减的详细说明和正当性理由。</p> <p>ISMS 的方针：（1）设定 ISMS 目标的框架和建立信息安全工作的总方向、原则；（2）考虑业务和法律、法规的要求，以及合同中的安全义务；（3）在组织的战略性风险管理的环境下，建立和保持 ISMS；（4）建立风险评价的准则。</p>	

续表

控制项	网络安全认证、检测及风险评估法规遵从建议	对应条款
计划（Plan）	<p>风险评估和管理在准备阶段主要包括以下工作：明确将本组织的信息安全管理纳入风险评估，制定接受风险的准则，识别可接受的风险级别。主要要求包括：识别 ISMS 范围内的资产和责任人；识别资产面临的威胁；识别可能被威胁所利用的资产脆弱性；识别丧失保密性、完整性和可用性之后可能对资产造成的影响；根据主要的威胁、脆弱性、对资产的影响及当前所实施的控制错误，评估安全实效发生的现实可能性；估计风险的级别；确定风险是否可以接受，是否需要按照组织所确定的风险接受准则来处理；采取适当的控制措施以降低或规避风险；在明显满足方针策略和接受风险准则的条件下，有意识客观地接受风险；组织的管理者应对本组织的残余风险有所了解。</p> <p>适用性声明主要包括三方面的准备：（1）上述选择的控制目标和控制措施；（2）当前的控制目标和控制措施；（3）对任何控制目标和控制措施的删减，以及删减的合理说明</p>	
实施（Do）	主要包括七方面：制订风险控制计划；实施风险控制计划；度量所选择的控制措施的有效性；实施培训意识和教育计划；实施安全事件响应计划；管理 ISMS 的运行；管理 ISMS 的资源	
检查（Check）	主要包括四方面的内容：ISMS 的执行程序及其他控制措施是否得以认真贯彻落实；是否对 ISMS 的有效性定期评审；度量控制措施的有效性以验证安全要求是否得到满足；是否按照计划的时间间隔进行风险评估的评审	
处置（Act）	实施已发现的 ISMS 需要改进的措施； 从其他组织或组织自身的安全经验中汲取教训； 与所有相关方沟通执行措施和改进措施情况； 确保改进达到了预期目标	

表 8-3 为《网络关键设备和网络安全专用产品目录（第一批）》内容。

表 8-3 《网络关键设备和网络安全专用产品目录（第一批）》

	设备或产品类别	范围
网络关键设备	1. 路由器	整系统吞吐量（双向）≥12Tbps 整系统路由表容量≥55 万条
	2. 交换机	整系统吞吐量（双向）≥30Tbps 整系统包转化率≥10Gpps

续表

	设备或产品类别	范围
网络关键设备	3. 服务器（机架式）	CPU 数量≥8 个 但 CPU 内核数≥14 个 内存内量≥256GB
	4. 可编程逻辑控制器（PLC 设备）	控制器指令执行时间≤0.08 微妙
网络安全专用 产品	5. 数据备份一体机	备份容量≥20T 备份速度≥60MB/S 备份时间间隔≤1 小时
	6. 防火墙（硬件）	整机吞吐量≥80Gbps 最大并发连接数≥300 万 每秒新建连接数≥25 万
	7. WEB 应用防火墙（WAF）	整机应用吞吐量≥6Gbps 最大 HTTP 并发连接数≥200 万
	8. 入侵检测系统（IDS）	满检速率≥15Gbps 最大并发连接数≥500 万
	9. 入侵防御系统（IPS）	满检速率≥20Gbps 最大并发连接数≥500 万
	10. 安全隔离与信息交换产品（网闸）	吞吐量≥1Gbps 系统延时≤5ms
	11. 反垃圾邮件产品	连接处理速率（连接/秒）>100 平均延迟时间<100ms
	12. 网络综合审计系统	抓包速度≥5Gbps 记录事件能力≥5 万条/秒
	13. 网络脆弱性扫描产品	最大并行扫描 IP 数量≥60 个
	14. 安全数据库系统	TPC-E tpsE（每秒可交易数量）≥4 500 个
	15. 网站恢复产品（硬件）	恢复时间≤2ms 站点的最长路径≥10 级

## 第 9 章

# 网络安全信息披露

伴随互联网和信息化的迅猛发展，网络安全对国家经济、社会生活甚至国家安全的影响日益增强。与此同时，银行、电信网络、政府部门等关键基础设施、大型商业网站、云服务、工业控制系统均日益成为网络攻击重点；基础网络、重要信息系统、通用软硬件的漏洞攻击风险、大型网站数据和个人信息泄露现象严重，网络安全事件频发，信息披露诉求应运而生。2016 年我国某“白帽子”披露世纪佳缘网站漏洞引发刑事立案，2017 年相继发生的 WannaCry 勒索病毒全球攻击事件引发全球各界对信息披露制度的重新思考，网易向未经授权擅自公开披露漏洞信息细节的某“白帽子”发公开声明，国家信息安全漏洞共享平台 CNVD 公告称因漏洞的不当披露引发党政机关和重要行业网站受到大规模攻击威胁等事件则进一步彰显了网络安全漏洞不规范或非法披露的现实冲击，网络信息的不当披露引起的法律后果等问题成为法律和行业界共同关注的焦点。以下将以《网络安全法》为背景，对网络安全信息披露的法规遵从做出具体的分析。

### 第一节 《网络安全法》相关规定及释义

网络安全信息披露，又称网络安全信息发布，我国《网络安全法》对于网络安全信息披露制度做出了相关规定，与之相关的法条包括：《网络安全法》第二十

六条规定：开展网络安全认证、检测、风险评估等活动，向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息，应当遵守国家有关规定。该条款规定的是两个并列行为，即：①开展网络安全认证、检测、风险评估等活动；②向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息，这两个行为都必须遵守国家有关规定，违反其中一个行为就会受到惩罚。该条没有限定主体，但从《网络安全法》章节设置、上下文条款内容以及实践中发布信息的主体来说，该条规制的主体包括任何组织和个人。

从现行实践观察，披露网络信息的常见主体包括：①政府机构，例如，国家互联网应急中心等；②开展网络安全认证、检测、风险评估等活动的机构；③第三方漏洞管理平台，例如，我国的补天平台、美国的 Hackerone 等；④个人，这里的个人在实践中一般多为黑客、“白帽子”等具有技术能力的人员。披露信息与发现信息的一般为同一个人。披露信息需要遵守的国家有关规定包括《保守国家秘密法》、《刑法》、《国家安全法》、《突发事件应对法》、《国家突发公共事件总体应急预案》等。从披露客体来看，若网络信息属于国家秘密、关键信息基础设施漏洞信息等，则不能进行披露；从披露主体来看，若披露主体为第二种时，即开展网络安全认证、检测、风险评估等活动的机构，还要遵守《合同法》，对于双方约定的不能披露的信息，应严格遵从合同内容的约定。

## 第二节 网络安全信息披露制度概述

近年来，利用网络安全漏洞、计算机病毒等实施攻击的安全事件在全球范围内频发，给网络空间安全带来了不可逆的危害。网络信息披露已成为网络安全风险控制的中心环节，对于降低风险起着至关重要的作用。强化网络信息收集、分析、报告、通报等在内的风险预警和信息通报工作已成为国家网络安全保障的重要组成部分。向不特定的社会公众披露网络信息可以提升网络安全防护的实时性和有效性，但恶意或非法的网络信息披露同样为攻击者提供了可利用的攻击武器。漏洞等网络信息发现之后是否应该披露，应该由谁披露，怎样披露，何时披露等问题变得日益

复杂且重要。出于国家安全和公共利益的现实考虑，网络信息披露应当遵循特定的规则，这种规则在美国立法中规定得较为完善，我国立法相对零散。

## 一、网络安全信息披露的界定

《网络安全法》第二十六条通过列举方式界定了网络安全信息的一般范围，包括系统漏洞、计算机病毒、网络攻击、网络侵入等，这是从网络安全信息技术类型角度的定义，体现了网络安全信息承载网络安全风险的基本功能。系统漏洞作为第一位的网络安全信息，是导致网络安全风险和产生网络安全事件的主要原因之一。但网络安全风险并不意味着必然发生网络安全事件。就安全漏洞而言，漏洞发现导致网络安全风险的产生，但只有进一步的漏洞披露，才将潜在的网络安全风险变成了现实的网络安全事件。网络安全信息披露本身可以被视为将风险信息公知化的过程，但基于网络安全信息的敏感性，这一公知过程可能产生潜在的负面影响。为此，网络安全信息披露需要在有效机制的规范下予以实施。网络安全信息披露机制是网络安全事件信息披露的约束性框架，是对可能造成特定信息系统和信息内容安全减损、影响用户合法权益、造成人身或财产损失，或者可能产生其他严重危害后果的事件信息进行公知活动的系统性规范，包括披露主体、披露内容、披露程序、披露时间、披露对象、相关责任和例外规定等，进而有效规范网络安全信息披露活动。

## 二、网络安全信息披露机制的作用

网络安全信息披露机制对于防范和控制网络安全风险具有重要作用。国家互联网应急中心（CNCERT）报告显示，仅2015年8月就收到网络安全事件达9655起<sup>①</sup>。诸如针对信息系统的安全威胁：2014年“全国DNS大劫难”事故中超过85%的用户遭遇了网速变慢和网站打不开的DNS故障，国内2/3网站因此受影响；美国《福布斯》网站报道一款漏洞“可被黑客利用在不被检测情况下实现对全球八

<sup>①</sup> 国家互联网应急中心. CNCERT 互联网安全威胁报告, 2015.

成个人计算机、网络应用或者云端虚拟机实现监控”<sup>①</sup>。另据国家互联网应急中心 2016 年第 39 期发布的互联网安全威胁报告显示, 仅 2016 年 9 月 19 日至 25 日一周内“境内感染网络病毒主机数 59.1 万; 网站被篡改数量为 2 477 个, 包括政府网站 53 个; 新增信息系统安全漏洞 257 个, 其中, 高危漏洞 146 个; 处理各类网络安全事件 622 起, 包括跨境案件 158 起”<sup>②</sup>。有鉴于此, 频发的网络安全事件无论是针对网络运行系统安全, 还是网络信息内容安全都已成为关乎互联网健康发展乃至国家和社会稳定的重大问题, 而有效的网络安全治理机制尤显必要和紧迫。鉴于网络安全风险和威胁的动态性, 目前的网络安全事件治理缺乏一种动态的机制以实现对网络信息安全事件的前期控制, 而网络安全事件信息披露机制的建构即可体现“预防与控制”的理念。面对不断增长的网络安全事件威胁, 确立有效的信息披露机制可使用户及时预判, 并因此而防范和控制风险和威胁的产生, 以保障网络信息安全。

### 三、美国网络安全信息（漏洞）披露制度的法律规定

在网络安全立法和实践始终处于领先地位的美国, 网络安全漏洞披露作为整个信息披露的关键一环, 早已引起法律和政策上的广泛关注。鉴于漏洞带给计算机信息系统的危害日益增加, 美国关于信息披露的立法较多, 这里以漏洞信息披露的法律规定为核心研究对象。美国法律框架下的网络安全漏洞披露规则主要体现在 2015 年的《网络安全信息共享法》(Cybersecurity Information Sharing Act, CISA)、2016 年的《商业与政府信息技术和工业控制产品或系统的漏洞裁决政策和程序》(Vulnerability Equities Process, VEP) 及《2017 补丁法案》中。

#### (一)《网络安全信息共享法》

《网络安全信息共享法》是美国关于网络安全信息共享的第一部综合性立法,

① 佚名. 美发现新浏览器攻击模式: 可监控全球八成 PC[EB/OL]. [2015-04-24]. [http://www.cnnic.net.cn/gjymaqzx/aqgg/aqggaqsj/201504/t20150424\\_52123.htm](http://www.cnnic.net.cn/gjymaqzx/aqgg/aqggaqsj/201504/t20150424_52123.htm).

② 国家互联网应急中心. 网络安全信息与动态周报 (2016 年第 39 期) [EB/OL]. [2016-09-30]. <http://www.cert.org.cn/publish/main/upload/File/2016CNCERT39.pdf>.



也是奥巴马政府最重要的网络安全综合性立法成果。该法授权政府机构、企业以及公众之间可以在法定条件和程序下共享网络安全信息。CISA 将共享的网络安全信息分为“网络威胁指标”和“防御措施”两大类。网络威胁指标实质为直接的漏洞威胁和与漏洞相关的其他威胁，防御措施则是针对网络威胁指标做出的技术和其他措施的回应。总体来说，CISA 围绕“网络威胁指标”和“防御措施”建立了美国网络安全信息共享的基本框架。CISA 鼓励私企与美国政府实时共享网络安全威胁信息，特别规定了私主体共享信息的责任豁免；对于通过合法共享而获得的网络威胁指标和防御措施，联邦政府基于识别网络安全威胁或者安全漏洞的需要可以披露。

## （二）VEP 政策

奥巴马政府时期，美国联邦调查局、国家安全局等政府机构一方面通过采购、收集等方式进行网络安全漏洞的攻击性研究和储备，另一方面制定和施行 VEP 政策，评判收集到的漏洞对网络安全、信息保障、情报、执法、国防和关键基础设施保护的影响，裁决是披露已经获得或发现的安全漏洞，还是保留安全漏洞用于情报、执法或者其他目的。VEP 政策的整体内容在美国现行制度下仍属于“国家秘密”信息，直至 2016 年才向公众公布其中一部分。依据 VEP 政策的公开的规定，美国政府实体对于任何来源的网络安全漏洞信息裁决程序如下：第一，基于漏洞分级，在触发特定阈值时向国家安全局指定担任的执行秘书长通报；第二，执行秘书长通知政府相关的利益相关方，指定特定联络人，由各方反馈是否启动裁决程序；第三，提出裁决要求的所有利益相关方指派特定专家参与讨论，并向裁决审查委员会（Equities Review Board, ERB）提供决策建议；第四，裁决审查委员会做出如何响应漏洞的倾向性决定，如有利益相关方有异议，则该机构可向某特定内设机构提出申诉。

## （三）《2017 补丁法案》

为将 VEP 政策正式纳入立法范畴，进一步规范政府、厂商等披露主体的行为，同时解决 CISA 法案和 VEP 政策在安全漏洞信息共享和披露实施方面的衔接问

题，2017年5月17日，美国国会提出了一项新法案——《2017反黑客保护能力法案》，也被称为《2017补丁法案》。

总体来说，2017年补丁法案在“是否披露”和“如何披露”两个核心问题上体现出美国政府对VEP政策的改进。首先，补丁法案改变了漏洞披露裁决的顶层决策机制，实现了从国家安全局到国土安全部主导的过渡。补丁法案规定，由国土安全部长（或其指定人员）担任的“漏洞裁决审查委员会”主席代替VEP政策中国家安全局指定的执行秘书长，“漏洞裁决审查委员会”主席与联邦调查局、国家情报总监、中央情报局、国家安全局，以及商务部、国务院、财政部、能源部和联邦贸易委员会的指定人员等共同组成漏洞裁决审查委员会。这一决策主体的变化用意在于增加透明度，规避公众对国家安全局的敏感性。其次，补丁法案增加了推定披露程序。法案规定将通过制定标准，指引对推定披露程序的适用，以此弥合常规披露与“黑市披露”之间的时间差。但由于最终由国土安全部长代表联邦政府实施披露，所以其有效性仍有待观察和评估。再次，补丁法案加大了向厂商的安全漏洞披露倾向。法案规定，如果漏洞裁决审查委员会决定向特定厂商披露，则应当国土安全部长实施披露。此种情形属于向特定人的有限披露。最后，补丁法案规定，对于裁决禁止披露、但因任何原因进入公众领域的网络安全漏洞，应按照CISA制定的程序实施。

### 第三节 网络安全信息披露法规遵从框架及建议

#### 一、网络安全信息披露制度的法规遵从框架（见表9-1）

我国有关网络安全信息披露（发布）的直接立法较少且零散，主要体现在《网络安全法》、《国家安全法》、《突发事件应对法》和《国家突发公共事件总体应急预案》中，但是根据信息披露主体的不同，也应遵守《保守国家秘密法》、《合同法》和《刑法》等相关条款。

表 9-1 网络安全信息披露制度的法规遵从框架

法律法规名称	具体规定	颁布机构与颁布时间	法律状态
《网络安全法》	<p>第二十六条规定：开展网络安全认证、检测、风险评估等活动，向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息，应当遵守国家有关规定。</p> <p>第六十二条规定：违反本法第二十六条规定，开展网络安全认证、检测、风险评估等活动，或者向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息的，由有关主管部门责令改正，给予警告；拒不改正或者情节严重的，处一万元以上十万元以下罚款，并可以由有关主管部门责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处五千元以上五万元以下罚款</p>	全国人大常委会，2017-6-1	现行生效
《国家安全法》	<p>第六十七条规定：国家健全国家安全危机的信息报告和发布机制。国家安全危机事件发生后，履行国家安全危机管控职责的有关机关，应当按照规定准确、及时报告，并依法将有关国家安全危机事件发生、发展、管控处置及善后情况统一向社会发布</p>	全国人大常委会，2015-7-1	现行生效
《突发事件应对法》	<p>第三十七条规定：国务院建立全国统一的突发事件信息系统。县级以上地方各级人民政府应当建立或者确定本地区统一的突发事件信息系统，汇集、储存、分析、传输有关突发事件的信息，并与上级人民政府及其有关部门、下级人民政府及其有关部门、专业机构和监测网点的突发事件信息系统实现互联互通，加强跨部门、跨地区的信息交流与情报合作。</p> <p>第四十四条规定：发布三级、四级警报，宣布进入预警期后，县级以上地方各级人民政府应当根据即将发生的突发事件的特点和可能造成的危害，采取下列措施：（二）责令有关部门、专业机构、监测网点和负有特定职责的人员及时收集、报告有关信息，向社会公布反映突发事件信息的渠道，加强对突发事件发生、发展情况的监测、预报和预警工作。”第六十三条规定了相关的法律责任，“地方各级人民政府和县级以上各级人民政府有关部门违反本法规定，不履行法定职责的，由其上级行政机关或者监察机关责令改正；有下列情形之一的，根据情节对直接负责的主管人员和其他直接责任人员依法给予处分：（二）迟报、谎报、瞒报、漏报有关突发事件的信息，或者通报、报送、公布虚假信息，造成后果的</p>	全国人大常委会，2017-11-1	现行生效

续表

法律法规名称	具体规定	颁布机构与颁布时间	法律状态
《国家突发公共事件总体应急预案》	第 3.4 节规定了信息发布制度的原则和披露方式：突发公共事件的信息发布应当及时、准确、客观、全面。事件发生的第一时间要向社会发布简要信息。信息发布形式主要包括授权发布、散发新闻稿、组织报道、接受记者采访、举行新闻发布会等	国务院， 2006-1-8	现行生效
《中国互联网协会漏洞信息披露和处置自律公约》	第九条规定：漏洞平台应遵循的自律义务有建立规范的漏洞信息接收、处理和发布流程。对漏洞报送者提交的信息要进行预先核实，确保漏洞信息的真实性和完整性，以便于漏洞验证和核实；建立信息颁发处理机制，确保漏洞信息及时流转到处置环节；规范漏洞信息发布机制，建立与 CNCERT 联动的信息审核发布机制，加强对漏洞平台用户的管理，确保漏洞披露和扩散渠道可控可追溯。  第十一条规定了各方在漏洞信息披露方面应遵循“客观、适时、适度”三原则	行业协定， 2015-6-9	现行生效

二、网络安全信息披露的法规遵从建议

我国《网络安全法》第二十六条规定：开展网络安全认证、检测、风险评估等活动，向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息，应当遵守国家有关规定。第五十一条规定：国家建立网络安全监测预警和信息通报制度。国家网信部门应当统筹协调有关部门加强网络安全信息收集、分析和通报工作，按照规定统一发布网络安全监测预警信息。第六十二条规定：违反本法第二十六条规定，开展网络安全认证、检测、风险评估等活动，或者向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息的，由有关主管部门责令改正，给予警告；拒不改正或者情节严重的，处一万元以上十万元以下罚款，并可以由有关主管部门责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处五千元以上五万元以下罚款。《网络安全法》对于网络安全漏洞信息披露的披露过程、责任主体和法律责任做出了原则性规定，表 9-2 对具体的法规遵从及遵从建议做出了分析。

表 9-2 网络安全信息披露制度的法规遵从分析

控制项	网络安全信息披露的法规遵从建议	对应条款
开展认证、检测、风险评估活动与网络安全信息披露	网络安全信息披露主体（如开展认证、检测、风险评估活动的机构）在披露网络安全信息时应遵循公平、公正、公开原则，在规定时间内发布网络安全信息及修复措施。  网络安全漏洞发布应是在风险最小化的原则下有条件的公开，例如 Oday 漏洞不宜公开。  厂商应建立漏洞发布渠道，在规定时间内发布漏洞信息及修复措施，并通知用户。  漏洞处理时间为：验证不大于 10 个工作日；反馈不大于 5 个工作日；开发修复措施不大于 30 个工作日；漏洞通报管理组织不大于 5 个工作日；发布漏洞信息及修复措施不大于 5 个工作日	第二十六条规定：开展网络安全认证、检测、风险评估等活动，向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息，应当遵守国家有关规定

第四节 典型案例

实践中关于信息披露的案例较多，常见于安全漏洞信息披露或者政府机构的信息披露之中，在此列举两个典型案例，反应漏洞信息披露的主观意图、定罪量刑依据，以及政府信息披露发生的情况和披露内容。

一、Bret McDanel 善意发布 Tornado 公司漏洞信息案例

Bret McDanel 是 Tornado 开发公司员工，Tornado 开发公司是一家位于洛杉矶，提供网页邮件和语音邮件服务的公司。在工作过程中，Bret McDanel 发现了公司电子邮件系统的严重安全漏洞，该漏洞可让外界人员阅读客户的私人信息。McDanel 向上级反映，但漏洞并未得到修补。不久后，McDanel 离开了 Tornado 公司，去到另一家公司工作。

6 个月后，McDanel 得知 Tornado 公司并未对漏洞进行修补。之后 McDanel 向约 5 600 个 Tornado 客户发送匿名邮件。告知 Tornado 客户相关漏洞，并引导他们到他自己的网页上了解详细信息。他的目的在于尽量减少对 Tornado 电子邮件服务器的影响。

Tornado 公司得知邮件的消息后,在未获得客户许可的情况下立即删除了客户的邮件,以防止客户得知漏洞事宜。之后,他们采取了其他措施对漏洞进行隐蔽。最后,他们将漏洞进行了修补并对整体安全性进行了升级。

2002 年,McDanel 被定罪,被判处 16 个月联邦监狱监禁。没有证据证明 McDanel 或任何其他他人利用了该漏洞。为了判处 McDanel 监禁,政府对联邦电脑犯罪法案进行了独特的解释。根据《计算机欺诈与滥用法》中的相关条款:“有意进行程序、信息、代码或指令传播,并且由于上述行为,在未经授权情况下,故意对受保护的电脑造成损害”的行为属于犯罪行为。该法案旨在追究拒绝承认其进行服务攻击并向计算机发送多封电子邮件导致计算机崩溃的攻击者责任,该行为实际导致系统关闭并对计算机系统本身造成影响。

McDanel 服刑结束后,政府判定此前对他的起诉存在错误并撤销了他的定罪。在简报中,司法部律师写到,他们起先认为被起诉的 McDanel 涉及《计算机欺诈与滥用法》中“适当、诚信建立”罪。Ronald Cheng,美国加利福尼亚州中部助理律师在文档中写到:“政府承认,证据未证明其做法属于法案中故意“损坏”的定义,并要求法庭撤销被告人判决。”McDanel 的辩护律师 Jennifer Granick 补充到:“这起诉讼涉及政府认定 McDanel 是一个对其前雇主存在犯罪心理和动机的‘黑客’。其动机是 Tornado 拒绝对发现的安全问题进行修复,而 McDanel 就选择将情况告知客户,确保客户采取保护措施。这并非犯罪行为。”

## 二、关于防范 Windows 操作系统勒索软件 WannaCry 的情况通报

针对 2017 年 5 月风靡的勒索软件事件,我国国家互联网应急中心发布了官方通告,告知广大用户勒索软件的情况及能够采取的应急处置措施,这是根据《网络安全法》第二十六条规定展开的网络安全信息发布活动,有利于用户及时采取措施降低损失。国家互联网应急中心发布的相关通报如下。

5 月 12 日,互联网上出现针对 Windows 操作系统的勒索软件(WannaCry)攻击案例。勒索软件利用此前披露的 Windows SMB 服务漏洞(对应微软漏洞公告:MS17-010)攻击手段,向终端用户进行渗透传播,并向用户勒索比特币或其

他价值物，包括高校、能源等重要信息系统在内的多个国内用户受到攻击，已对我国互联网络构成较为严重的安全威胁。

### （一）勒索软件情况

综合国家互联网应急中心和国内网络安全企业（奇虎 360 公司、安天公司等）已获知的样本情况和分析结果，该勒索软件在传播时基于 445 端口并利用 SMB 服务漏洞（MS17-010），总体可以判断是由于此前“Shadow Brokers”披露漏洞攻击工具而导致的后续黑产攻击威胁。4 月 16 日，国家互联网应急中心主办的 CNVD 发布《关于加强防范 Windows 操作系统和相关软件漏洞攻击风险的情况公告》，对影子经纪人“Shadow Brokers”披露的多款涉及 Windows 操作系统 SMB 服务的漏洞攻击工具情况进行了通报（相关工具列表见表 9-3），并对有可能产生的大规模攻击进行了预警。

表 9-3 有可能通过 445 端口发起攻击的漏洞攻击工具

工具名称	主要用途
ETERNALROMANCE	SMB 和 NBT 漏洞，对应 MS17-010 漏洞，针对 139 和 445 端口发起攻击，影响范围：Windows XP、Windows Server 2003、Windows Vista、Windows 7、Windows 8、Windows Server 2008、Windows Server 2008 R2
EMERALDTHREAD	SMB 和 NETBIOS 漏洞，对应 MS10-061 漏洞，针对 139 和 445 端口，影响范围：Windows XP、Windows Server 2003
EDUCATEDSCHOLAR	SMB 服务漏洞，对应 MS09-050 漏洞，针对 445 端口
ERRATICGOPHER	SMBv1 服务漏洞，针对 445 端口，影响范围：Windows XP、Windows Server 2003，不影响 Windows Vista 及之后的操作系统
ETERNALBLUE	SMBv1、SMBv2 漏洞，对应 MS17-010，针对 445 端口，影响范围较广，从 Windows XP 到 Windows Server 2012
ETERNALSYNERGY	SMBv3 漏洞，对应 MS17-010，针对 445 端口，影响范围：Windows 8、Windows Server 2012
ETERNALCHAMPION	SMB v2 漏洞，针对 445 端口

当用户主机系统被该勒索软件入侵后，弹出如图 9-1 所示的勒索对话框，提示勒索目的并向用户索要比特币。而对于用户主机上的重要文件，如照片、图片、文档、压缩包、音频、视频、可执行程序等几乎所有类型的文件，都被加密的文件后缀名被统一修改为“.WNCRY”，如图 9-2 所示。目前，安全业界暂未能有效破除该勒索软的恶意加密行为，用户主机一旦被勒索软件渗透，只能通过重装操

作系统的方式来解除勒索行为，但用户重要数据文件不能直接恢复。



图 9-1 勒索软件界面图







	Hydrangeas.jpg.WNCRY	2009/7/14 12:52
	Jellyfish.jpg.WNCRY	2009/7/14 12:52
	Koala.jpg.WNCRY	2009/7/14 12:52
	Lighthouse.jpg.WNCRY	2009/7/14 12:52
	Penguins.jpg.WNCRY	2009/7/14 12:52
	Tulips.jpg.WNCRY	2009/7/14 12:52

图 9-2 用户文件被加密

## （二）应急处置措施

国家互联网应急中心已经着手对勒索软件及相关网络攻击活动进行监测，5月13日9时30分至12时，境内境外约101.1万个IP地址遭受“永恒之蓝”SMB漏洞攻击工具的攻击尝试，发起攻击尝试的IP地址（包括进行攻击尝试的主机地址以及可能已经感染蠕虫的主机地址）数量9300余个。建议广大用户及时更新Windows已发布的安全补丁更新，同时在网络边界、内部网络区域、主机资产、数据备份方面做好如下工作。

（1）关闭445等端口（其他关联端口如135、137、139）的外部网络访问权限，在服务器上关闭不必要的上述服务端口。

（2）加强对445等端口（其他关联端口如135、137、139）的内部网络区域



访问审计，及时发现非授权行为或潜在的攻击行为。

- (3) 及时更新操作系统补丁。
- (4) 安装并及时更新杀毒软件。
- (5) 不要轻易打开来源不明的电子邮件。
- (6) 定期在不同的存储介质上备份信息系统业务和个人数据。

国家互联网应急中心后续将密切监测和关注该勒索软件的攻击情况，同时联合安全业界对有可能出现的新的攻击传播手段、恶意样本进行跟踪防范。

## 第五节 监督管理与责任

《网络安全法》第八条规定：国家网信部门负责统筹协调网络安全工作和相关监督管理工作。国务院电信主管部门、公安部门和其他有关机关依照本法和有关法律、行政法规的规定，在各自职责范围内负责网络安全保护和监督管理工作。第六十二条规定：违反本法第二十六条规定，开展网络安全认证、检测、风险评估等活动，或者向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息的，由有关主管部门责令改正，给予警告；拒不改正或者情节严重的，处一万元以上十万元以下罚款，并可以由有关主管部门责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处五千元以上五万元以下罚款。

根据第八条规定，《网络安全法》规定了网络安全信息披露的监督管理制度，即“1+X”模式：国家网信部门负责统筹协调网络安全工作，国务院电信主管部门、公安部门和其他有关机关依照本法和有关法律、行政法规的规定，在各自职责范围内负责网络安全保护和监督管理工作。此外，违反《网络安全法》第二十六条规定的处罚措施包括：①责令改正。所谓责令改正或者限期改正违法行为，是指行政主体责令违法行为人停止和纠正违法行为，以恢复原状，维持法定的秩序或者状态，具有事后救济性。②警告。③罚款。拒不改正或者情节严重的，处一万元以上十万元以下罚款。④停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照。

## 第 10 章

# 协助执法

2013 年爆发的美国国家安全局监控丑闻，一度引发世界各国和民众的监听恐慌，国家安全与个人隐私的冲突使协助执法制度的时代张力凸显无疑。一贯被作为协助执法制度内涵核心的合法拦截和数据留存规定也因可能存在的隐私风险而被极力限制。近年来，恐怖分子和其他违法犯罪分子利用多种先进且安全性较高的网络信息通信工具逃避国家安全机关和公安机关的侦查和调查活动，宣扬恐怖主义、实施恐怖袭击和其他违法犯罪活动，对国家安全和社会稳定产生了巨大威胁。为此，对网络运营者附加必要的协助执法义务已经成为各国的通行做法。我国颁布的网络安全基础性保障法《网络安全法》重申了数据留存和技术支持制度，标志着协助执法制度成为网络安全上位法中的基本制度。

### 第一节 《网络安全法》相关规定及释义

2016 年 11 月 7 日，我国正式发布《网络安全法》，于 2017 年 6 月 1 日起实施，第二十一条和二十八条规定了数据留存和技术支持内容。这是我国首次在网络安全专门性和基础性保障法中规定协助执法制度，由此也可看出协助执法制度对于信息技术时代追查、打击犯罪的重要性。

《网络安全法》第二十一条规定国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：（三）采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月。根据第二十一条可知，《网络安全法》规定的协助执法义务主体是网络运营者，基本要求是按照网络安全等级保护制度的要求，进行数据留存，直接目的是保障网络免受干扰、破坏或未经授权的访问，防止网络数据泄露或被窃取、篡改，留存期限至少为六个月。这里并没有直接规定协助执法制度的权力主体，而是单纯以网络运营者义务的形式进行规定，但数据留存的要求本质上与协助执法义务一致，在公安机关等执法机构进行取证时，可以按照相应法律获取留存的数据。

相比第二十一条，《网络安全法》第二十八条规定网络运营者应当为公安机关、国家安全机关依法维护国家安全和侦查犯罪的活动提供技术支持和协助。该条规定直接体现了协助执法制度，规定协助执法的义务主体仍然是网络运营者，权力主体是公安机关、国家安全机关，目的是实现维护国家安全和侦查犯罪的活动，要求是提供技术支持和协助，这里的技术支持和协助既包括合法拦截也包括数据留存等有助于获取证据的措施。

协助执法制度的法律责任主要规定在《网络安全法》的第五十九条和第六十九条。第五十九条规定，网络运营者不履行本法第二十一条、第二十五条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处一万元以上十万元以下罚款，对直接负责的主管人员处五千元以上五万元以下罚款。第六十九条规定，网络运营者违反本法规定，有下列行为之一的，由有关主管部门责令改正；拒不改正或者情节严重的，处五十万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员，处一万元以上十万元以下罚款：（三）拒不向公安机关、国家安全机关提供技术支持和协助的。可以看出，承担责任的主体不仅包括网络运营者，还包括直接负责的主管人员，处罚方式包括责令改正、给予警告、罚款。一般情况是责令改正或警告，只有在拒不改正或情节严重时，才会进一步做出罚款的处罚。

## 第二节 协助执法制度概述

本节拟从协助执法的背景、概念、要求及国外相关规定、我国法规遵从等方面对制度本身进行解读。

### 一、《网络安全法》规定协助执法制度的背景

随着国家安全与利益之间的角逐日益白热化，为了打击恐怖主义和违法犯罪，秘密监控企业数据的丑闻也频繁曝光，使得监听的合法性引起激烈的立法讨论。2015 年雅虎秘密开发了一个定制软件程序，用于搜索全部用户所收到的实时电子邮件，目的是查找由美国情报官员向其提供的特定信息。2016 年 1 月，德国情报机构 BND 已经与美国国家安全局合作，从事间谍行动。同月，美国 FBI 承认运营儿童色情网站“钓鱼执法”。虽然美国官员承认“钓鱼执法”网站确实存在风险，但他们认为除此之外，没有其他方式可以追踪到访问这些网站的人员。参与了此前类似行动的 FBI 前高级官员罗恩·霍斯克（Ron Hosko）表示：“我们获得了一扇机会的窗口，以深入到地球上最黑暗的地方。如果不这样做，那么我们别无他法。”2016 年 2 月，根据达成的一项初步双边协议，美英两国的警方及情报机构，将被允许到对方国家的媒体公司，直接查询本国被调查人的电邮、聊天记录。

2016 年 10 月，雅虎秘密搜索用户电邮为美国安全官员提供信息的消息暴露。同月，英国调查权力法庭（Investigatory Powers Tribunal）宣判，英国间谍机构政府通信总部（GCHQ）曾在 1998—2015 年期间非法收集普通民众的个人信息，违反了《欧洲人权公约》第八条的规定，侵犯了英国公民的隐私。2013 年爱德华·斯诺登向媒体爆料 GCHQ 开展的窃听计划，范围比美国国家安全局进行的监控计划有过之而无不及<sup>①</sup>。2017 年美国国家情报总监办公室公布的报告显示，即使国会已经出台了遏制国家安全局大规模收集电话记录的新法系统，但是这个机构仍旧在 2016

---

<sup>①</sup> 发表于 2016 年 10 月 18 日，链接为 <http://digi.163.com/16/1018/10/C3LFU94U001687H3.html>。

年收集了 1.51 亿多条美国公民的电话记录。然而美国法院在 2016 年仅针对 42 名恐怖主义嫌疑人下达了使用电话收集系统的指令<sup>①</sup>。

即使 2013 年的棱镜门及系列监控事件引起了全球范围内对美国行为的激烈争议和谴责，但不论是美国，还是英国、德国等国家对数据的监控从未停止过，且大部分行为都是打着维护国家安全或侦查犯罪的旗号进行的暗箱操作。鉴于恐怖袭击的日益增多和损害后果的不可逆转，世界各国都在寻求监听的合法性和数据留存期限的合理性。例如，2015 年美国《自由法案》对广泛的合法拦截保持不变，同时对披露数据和透明度进行了调整；2016 年俄罗斯通过《反恐法修订案》，将数据留存的期限延长至三年；澳大利亚修订了《电信（监控和接入）修正（数据留存）案》，将数据留存规定为两年；英国的《调查权法案》更是规定了全面严格的合法拦截制度。在世界各国掀起协助执法制度立法研制的新一轮高潮的同时，我国《网络安全法》也针对国情，在现有立法基础上进一步规定数据留存和技术支持，符合时代趋势，对预防犯罪、维护公民合法权益和公共安全具有重要作用。

## 二、协助执法的概念分析

传统法律意义上的协助执法制度，是指执法机构在进行侦查和刑事调查时，相关的单位和个人有义务提供执法便利。鉴于网络的普及和对基础设施的渗透影响，协助执法一般被理解为通信协助执法。因此，提供执法便利应当作广义理解，即有助于侦查和调查的协助行为都应当包含在协助执法的范畴之内。通信协助执法首先是针对通信服务提供者和电信设备制造商等。1994 年美国通过《通信协助执法法》以立法名称的形式正式使用“通信协助执法”这一概念，该法要求某一指定电信部门通过对其系统进行设计或更新，从而确保有权的监控机关获取监控信息用以履行职责。追查犯罪时，协助执法是每个公民和组织的法定义务，传统的方式包括举报犯罪、协助司法机关进行犯罪调查等。在现代信息化社会，协助执法早已超越传统的举报犯罪等协助方式，衍生出新的形式，即需要电信服务提供者配置有关拦截的接口、设施（被称之为“合法拦截”），根据本国立法要求，

<sup>①</sup> 发表于 2017 年 5 月 3 日，链接为 <http://digi.163.com/17/0503/11/CJGPK2NF001687H3.html>。

保存表明用户活动的流量信息或位置信息一定时期（数据留存），通过对实时数据和存储数据的综合获取以协助执法。

合法拦截（Lawful Interception，动态）和数据留存（Data Retention，静态）成为各国常用和主要的协助执法方式。合法拦截，是指经法定授权的执法机构或者网络服务提供者基于维护国家安全或侦查刑事犯罪目的而采取技术手段获取通信内容或通信相关数据的活动。在信息通信技术泛在化利用的情况下，成为预防恐怖主义或其他犯罪活动的有效方法，也是刑事调查、侦查和起诉犯罪行为的重要手段。合法拦截的过程可以由侦查机关直接实施，也可以通过通信服务提供者协助实施。而这种实施的过程对于被拦截对象而言，属于秘密的侦查过程，所以对于通信服务提供者而言，应当满足一定的保守秘密的要求。数据留存旨在建立一个复杂的国家级监管计划，是指为保护国家安全、防务、公共安全而要求公共通信网络或公共电信服务提供者存留流量数据和位置数据一定时间，以协助执法单位进行严重犯罪与恐怖嫌犯之调查时参考利用。

综上，本书提出的协助执法为网络环境下广义的协助执法，可界定为通信服务提供者通过对自身设备进行特殊设计，以满足执法机构对特定对象的监控，其方式包括合法拦截和数据留存等，以进行协助预防和侦查犯罪、反恐怖主义等维护国家安全的行为<sup>①</sup>。

### 三、协助执法的主体和原则

#### （一）主体

协助执法活动通常是基于维护国家安全和便利刑事调查的目的，在执法机构不能独立进行刑事调查的情况下，由协助执法义务主体在收到法院授权、执法机构请求或者命令的情况下，利用自身的技术、人员和物质条件协助执法机构获取所需信息内容的过程。一般而言，协助执法的权力主体包括国家安全机关、情报机关、公安机关等，例如，美国包括国家安全局、联邦调查局等；澳大利亚包括情报机关、国家警察部队、澳大利亚犯罪委员会等；俄罗斯包括国家侦查机关、

---

<sup>①</sup> 马民虎，果园，网络通信监控法律制度研究[M]，北京：法律出版社，2013。

俄联邦安全机关等；我国则为公安机关和国家安全机关。此外，根据《刑事诉讼法》第一百四十八条规定，对于重大的贪污、贿赂犯罪案件以及利用职权实施的严重侵犯公民人身权利的重大犯罪案件，人民检察院在立案后可以采取技术侦查措施，按照规定交有关机关执行。

鉴于网络服务提供者在信息获取方面的绝对控制力和便利性，各国协助执法的义务主体通常为网络服务的提供者，除传统电信业务经营者之外，还包括网络电话服务提供者、虚拟电信运营者、网络信息服务提供者等多种新型网络服务提供者。概括而言，可以分为三类（见表 10-1）。

表 10-1 协助执法义务主体

主体	英文名称	我国对应概念	含义
网络运营商	Network Operator	基础电信运营商	通过有线、微波、光学手段或者其他（电磁的）方式在规定的网络终端点之间传输信号的公共电信基础设施的运营者
接入服务商	Access Provider	互联网接入服务提供者	向某些网络用户提供从用户终端到网络接入服务的主体
服务提供商	Service Provider	网络服务提供者	网络服务提供者可以向用户提供一个或者多个信息通信服务，但并不强制要求网络服务提供者自身运营或者拥有自己的网络

根据我国《反恐怖主义法》的规定，我国的协助执法主体包括电信业务经营者<sup>①</sup>和互联网服务提供者<sup>②</sup>。同时根据我国《网络安全法》的规定，协助执法主体为网络服务提供者，即网络的所有者、管理者和网络服务提供者，涵盖了上述三类协助执法义务主体，与国际通行做法保持一致。

## （二）原则

协助执法是在非正常渠道下获取通信信息的过程，尽管其以维护国家和社会稳定为价值目标，但超出权力边界的协助执法活动仍然存在侵犯公民通信秘密和个人隐私的风险。“棱镜门”事件所披露的美国执法机构大规模监听事实已然引发了侵犯个人隐私的强烈声讨，使协助执法制度的正当性受到严重影响。为防

① 根据我国《电信条例》的规定，电信是指利用有线、无线的电磁系统或者光电系统，传送、发射或者接收语音、文字、数据、图像以及其他任何形式信息的活动。电信业务经营者即从事上述活动的经营者。

② 根据我国《互联网信息服务管理办法》的规定，互联网信息服务是指通过互联网向上网用户提供信息的服务活动。互联网信息服务提供者即从事上述服务活动的提供者。

止权力滥用，各国均要求实施协助执法需要遵循必要的原则，包括适当性原则、必要性原则和均衡原则。

适当性原则又称适合性原则，是指协助执法活动应当以维护国家安全和便利刑事调查为目的，需要符合严格的程序规定，不能任意行使。

必要性原则要求协助执法在同等有效的措施中选择对公民权利损害最小的方法，不可过度干预公民的合法权益。必要性原则要求在实施协助执法前审查是否存在合法必要的前提，判断协助执法是否为执法机构所能采取的最后一种措施。

均衡原则又称相称性原则，是指协助执法所损害的利益应当小于其所保护的利益。为此，协助执法制度应当实现必要的利益平衡，综合考虑协助执法活动对个人隐私、产业发展和科技进步产生的潜在影响，设置合理的协助执法义务边界。如果协助执法义务设置过轻，将导致执法活动无法及时有效地完成，不能实现维护国家安全和便利刑事调查的目的；如果协助执法义务设置过重，则会对协助执法义务主体产生负担，不利于产业发展和技术创新，也会出现执法权力过大而侵犯个人隐私的不利后果。

## 四、协助执法内容及国外相关规定

目前，各国的协助执法内容主要依靠赋予网络服务提供者强制性的协助执法义务来实现，主要包括合法拦截、数据留存两大基本内容。随着 2016 年发生的圣伯纳迪诺市枪击案不断进入白热化，苹果与 FBI 的争议也引起了世界各国的争论，协助解密义务又被立法提上日程。鉴于加密已经成为互联网服务提供者的法定义务，而执法机关的解密能力会受到技术水平等条件的限制，协助解密也成为协助执法的重要内容，了解国外相关规定对完善我国协助执法法律制度具有借鉴意义。

### （一）合法拦截

根据各国协助执法的相关规定，协助执法义务主体在协助实施通信合法拦截时需要确立和维持执法机构的通信拦截能力。对信息通信设备进行改造或者升级，以确保执法机构的通信拦截能力是有效实施协助通信合法拦截的基础性要求，协助执法义务主体在新业务运营之前应保证其信息通信设备具备相应的通信合法拦



截能力。例如，法国的《邮电法》（Posts and Telecommunications Code）第 D98-1 章要求通信服务提供者与执法机构合作展开通信合法拦截，通信服务提供者应该安装拦截需要的技术设备并保证其可用。为了满足协助通信合法拦截的义务要求，协助执法义务主体通常需要进行以下通信设备和其他资源的改造或升级。一般而言，合法拦截的要求至少包括接口建设、建立实时的合法拦截能力、建立通信合法拦截的持续性能力、建立人员能力。

### 1. 接口建设

我国《反恐怖主义法》已经对接口建设做出了明确规定，要求电信业务经营者、互联网服务提供者公安机关、国家安全机关依法进行防范、调查恐怖活动提供技术接口。根据英国 2002 年《调查权法案（维持监听能力）的法令》[Regulation of Investigatory Powers (Maintenance of Interception Capability) Order] 的规定，“服务商应确保拦截的通信内容和通信相关数据传输至执法机构提供的交换接口，满足国务大臣提出的适当的协商一致并可行的行业技术标准要求”。通信拦截接口被称为 HI（Handover Interface），采用逻辑上相互独立的三端口结构，包括作为管理接口的管理信息接口（HI1）、作为技术接口的信息拦截接口（HI2）和通信内容接口（HI3）。

### 2. 建立实时的合法拦截能力

实时的合法拦截能力是实施协助通信合法拦截的主要内容，要求协助执法义务主体能够向执法机构提供有效的通信合法拦截途径或方法，以获取执法机构希望获得的通信信息或数据。例如，欧盟早在 1995 年 1 月 17 日的《关于通信合法拦截的委员会决议》（Council Resolution of 17 January 1995 on the lawful interception of telecommunications）中明确规定，服务商在接到授权通信合法拦截请求的一日内，应当提供实施合法拦截的有效途径。美国《通信协助执法法》（Communication Assistance for Law Enforcement Act）也要求运营商建立适当的策略和程序，保证拦截的数据能够传输到执法机构，并保证数据的安全性和完整性。

### 3. 建立通信合法拦截的持续性能力

在通信合法拦截的实施期间，协助执法义务主体必须确保其拦截设备具备持续性运行的能力。在出现拦截设备故障或拦截措施中断的情况下，应当及时向授

权机构进行通知，并说明故障或迟延的原因及其对通信合法拦截措施的影响。在恢复通信合法拦截能力之后，应当及时恢复正在进行的通信合法拦截，并通知授权机构。

#### 4. 建立人员能力

通信合法拦截具备专业性，协助执法义务主体除满足相关技术要求外，还需要提供必要的人员协助。例如，德国 2005 年的《通信拦截条例》（Telecommunications Interception Ordinance）第十二条第三款规定：义务当事人必须确保其拥有有资质的人员，能够在任何时候针对合法拦截措施中的技术执行问题接受授权机构的咨询。

### （二）数据留存

洛卡德认为，任何犯罪从本质上看都是一个物质间相互交换的过程，这种交换必然留下一定的痕迹，犯罪中的物质交换是不以人的主观意志为转移的。<sup>①</sup>信息社会，几乎任何人都与手机、电脑等通讯设施发生接触并留下大量数据，数据留存的目的就是快速获取相关数据，查找犯罪嫌疑人的行踪，提高执法便利，减少执法机构获取犯罪信息的障碍从而增加案件侦破的效率。与数据留存最相冲突的就是隐私保护，欧盟 2014 年废除了《数据留存指令》，原因就是觉得其侵犯了个人的自由和尊严，但欧盟的这种做法并没有引起其他国家的效仿。随着恐怖主义袭击频率增加和黑客犯罪技术的提高，证据更加难以溯源和跟踪，鉴于此，澳大利亚、俄罗斯等国反而在新的立法中增加了数据留存的期限。

一般而言，在各国立法中对数据留存的要求包含留存的义务主体、获取数据的权力主体、留存期限、留存的数据类型等。随着企业对数据库的投入和维护成本增加，某些国家立法开始明确对数据留存的补偿规定。留存的义务主体及权力主体与协助执法相同，留存期限一般包括六个月、一年、两年或三年等。对于留存的数据类型，不同的国家规定也不同，大部分与通信数据有关，例如通话时间、电子邮件发送时间等，为了保护隐私，一般不要求留存涉及通信具体内容的数据。

欧盟 2006 年《数据留存指令》颁布后，欧盟成员国都对其进行了国内转化立法，关于数据留存的期限，英国、芬兰、荷兰、法国、西班牙、意大利（限于互

<sup>①</sup> 周朋飞，李荣富.数据留存的必要性与可行性研究[J].辽宁警专学报.2014（1）：67.

联网接入、电子邮件和电话数据）规定为一年时间，卢森堡、立陶宛等国家规定为六个月。

2015年4月13日，澳大利亚通过《电信（监控和接入）修正（数据留存）法案》，对1979年的《电信（监控和接入）法案》及1997年的《电信法案》进行修正，规定澳大利亚安全情报组织、国家警察部队、澳大利亚犯罪委员会等20多个机构可以在没有令状的情况下查看通信元数据，要求电信运营商对特定类型电信数据的法定留存义务，留存期限为两年。通信数据（元数据）包括电话呼叫和互联网数据，电话呼叫包括：来电显示；通话的日期、时间和持续时间；通信位置或使用通信的路线；电话被分配的唯一标识符。网络数据包括：发送电子邮件的地址；电子邮件的发送日期、时间和接收人；电子邮件的附件大小和文件格式；互联网服务提供商（Internet Service Provider, ISP）持有的账户详细信息，例如账户是否已激活或暂停。服务提供者必须使用加密措施保护元数据的可信性，确保其免受未经授权的干扰和访问。

2016年6月24日，俄罗斯通过了《“反恐法”和在个别法律法规中确立反恐和社会治安补充措施的修正案》（简称《反恐法修正案》），补充《信息、信息技术与信息保护法》第三十一条规定：在互联网传播信息的组织者必须按照俄联邦法律规定的情形，向国家侦查机关或者俄联邦安全机关提供本章第三条规定的信息。其第三条规定为在互联网传播信息的组织者在俄罗斯境内必须保存：①关于互联网用户接收、转交、送达和（或）处理语音信息、文本、图像、声音、视频和其他电子信息事实数据，以及这些用户的信息，自行为实施一年以内；②互联网用户的文本信息、语音信息、图像、声音、视频以及互联网用户的其他电子信息，自信息接收、传递、送达和（或）处理起保存至六个月。保存上述信息的程序、期限和规模由俄联邦政府规定。同时，对《通信法》第六十四章第一条做出修订，通信运营商在俄罗斯境内必须保存：①有关通信用户接收、传递、送达和处理语音信息、文本信息、声音、视频或其他信息的事实数据，自行为实施三年以内；②通信用户的语音信息、文本信息、声音、视频或其他信息的数据，在接收、传递、送达和（或）处理六个月内。保存上述信息的程序、期限和规模由俄罗斯联邦政府规定。

近些年，随着网络的普及应用，个人、企业及其他数据呈指数增长，企业建

立数据库及维护数据库以遵从法律规定的年支出也不断递增,这对于互联网企业,尤其是处于发展初级阶段的中小企业来说是更加沉重的负担。

为了减轻企业的守法成本,更好地进行证据收集,一些国家规定了对数据留存的一些补偿措施。英国 2009 年《数据留存法》第十一条规定了国务大臣对公共通信提供者因遵守协助执法制度所支出的任何费用进行补偿的权力,但需事先通知国务大臣并征得同意,国务大臣拥有审计的权力。针对大部分 ISP 没有能力或成本过高构建数据留存系统的情况,2016 年 8 月,澳大利亚政府拨款 1.28 亿澳元作为数据留存的补偿款,对于那些遵守法律规定进行数据留存的企业,通过资金支持的方式减轻其守法成本,尤其强调对小型提供商的政策支持。获得资助的包括 180 个 ISP,大部分 ISP 获得了实施成本 80% 的补偿金,ISP 在签署资金协议时将立即获得其资金的 50%,以便帮助企业实现合规。在这次的资助计划中,最少的 ISP Arris 获得 1 万澳元,最多的是 ISP Telstra 获得 3 990 万澳元。

### (三) 协助解密

为了保证通信内容的安全性,越来越多的网络服务提供者开始使用密码技术提供通信加密服务。密码技术的核心原理是通过具体的算法将原文转换成密文,使通信内容对除密钥持有者以外的所有人具有“不可读性”。在通信信息进行加密的情况下,即使执法机构获取了通信信息,也无法获知其具体内容,使通信合法拦截失去应有的意义。为此,各国在协助执法的相关规定中,同样对协助执法义务主体附加了协助解密的要求。

目前,针对协助解密存在两种立法态度,一是遵循“谁运营,谁解密”原则,即协助执法义务主体应负责对其运营业务过程中所涉及的所有加密信息和数据进行解密;二是遵循“谁加密,谁解密”原则,即协助执法义务主体只负责对其自身进行加密的信息进行解密。考虑到密码技术的社会化利用,用户自行对通信信息进行加密,再通过网络服务进行存储、处理和传输的情况越来越普遍。在用户自行进行加密或持有密钥的情况下,网络服务提供者只是提供了通信信息存储、处理和传输的载体或渠道,并没有信息解密的能力。为此,各国普遍采用“谁加密,谁解密”的协助解密原则,只要求协助执法义务主体在其相应的能力范围内承担协助解密义务。只有在协助执法义务主体对通信信息进行编码、压缩或加密

时，才需要以明文形式向执法机构提供合法拦截获得的信息或提供可将加密信息转化为明文的工具，不包括用户自行加密的情况。

协助解密义务作为协助执法的重要组成部分，已经在多个国家立法中有所体现。

欧盟委员会在 1995 年通过《关于通信合法拦截的决定》(Council Resolution of 17 January 1995 on the Lawful Interception of Telecommunications)，经各成员国达成协议，发布执法机构与合法的协助执法有关要求。这些要求符合成员国内法，并应当遵循现行的国家政策。在该公告中，欧盟赋予各国的执法机构对网络运营/服务提供者提出了协助执法的要求，执法机构有权要求网络运营/服务提供者：①提供一个或多个接口，以确保拦截通信能够传输至执法机构的监控设备。接口必须经由拦截权力机构和网络运营/服务提供者的同意。其他相关事宜应当按照各国通行的方式处理。②如果网络运营/服务提供者对通信信息进行编码、压缩或加密，执法机构要求网络运营/服务提供者提供监控通信的明文。

法国 1991 年 7 月 10 日通过第 91 - 646 号法律《电信通信保密法》(Loi Sur Le Secret Des Correspondances, Law No. 91-646)，也被简称为《1991 法案》，其中第 11-1 章规定，通信服务提供者有义务提供加密信息的解密版本或者向有关当局提供解密密钥。

2000 年荷兰《互联网流量通信监控功能规范 (WAI 功能规范)》(Functional Specifications for Lawful Interception of Internet Traffic in the Netherlands) 规定，网络运营商或者通信服务提供者应当帮助解除任何应用在通信内容或者监控相关信息上的加密或其他密码服务，用普通文字提供监控结果。这意味着通信服务提供者的非常严格的协助解密义务，即无论加密服务是否由实施通信监控的通信服务提供者提供，都需要对已加密通信进行解密。

2004 年 6 月 22 日，德国议会批准了电信法遵从欧洲议会 2002 年 5 月的关于修改现有电信法的指令。根据 2004 年《电信法》(Telecommunications Act) 的第 110 节，要求通信服务提供者自费部署实施拦截必需的技术设施。

2004 年新西兰《电信 (拦截能力) 法》[Telecommunications (Interception Capability) Act] 规定，网络运营商必须以监察机关指定的格式 (以便可以解密) 收集呼叫相关数据和拦截电信。运营商还应确保该电信截取不干扰其他通信服务。

2016 年俄罗斯的《反恐法修正案》补充 2006 年《信息、信息技术与信息保护法》第四十一条规定“在互联网上传播信息的组织者，如果在接收、传递、送达和处理互联网用户电子信息时使用了电子信息附加加密，或者为互联网用户提供了电子信息附加加密的可能性，必须向联邦安全权力执行机关提供必要的接收、传递、送达和（或）处理的电子信息的解码信息”。

2016 年 11 月英国通过的《网络安全战略》提出，密码技术是保护敏感信息和国家安全的基础，且私有部门（企业）的技术和能力对于发展密码技术很重要。战略提到英国政府非常支持加密技术，因为加密可以保护公民的私人数据或知识产权，但与此同时英国也需要确保恐怖分子和罪犯不能借助加密来营造一个“安全空间”。英国政府希望和行业合作来确保这一点，并建立一个完善的法律框架和监管体系，警察和情报部门可以访问恐怖分子或罪犯间的通信内容。必要时，英国政府将要求企业对相关信息进行解密，而企业也需要配合政府进行解密<sup>①</sup>。

此外，协助执法是为维护国家安全和便利刑事调查而建立的制度，其主要特征在于协助执法过程的秘密性。如果协助执法活动或相关信息遭到泄露，就会使犯罪分子预先防备，采取规避措施，直接影响执法活动的有效性。为此，协助执法义务主体必须对协助执法过程中知悉的所有信息严格保密，包括协助执法活动本身的存在、获取的相关通信信息、执法主体、执法对象、执法期限等相关信息。

### 第三节 典型案例

近两年，因为协助执法引起纠纷的最出名的案件莫过于 2016 年美国发生的圣伯纳迪诺市枪击案，我国还未发生较大的因为协助执法引起纠纷的事例，目前为止，比较出名的协助执法案例大都与美国的企业有关，在此列举几个案例帮助了解实践中各方对协助执法的态度。

---

<sup>①</sup> 参考 <http://mt.sohu.com/20161111/n472968395.shtml>。

## 一、FBI 诉苹果公司案

2015 年 12 月，28 岁的赛义德·法鲁克（Syed RizwanFarook）和他 29 岁的妻子塔什芬·马利克（Tashfeen Malik）对加州的一家社会服务机构发起袭击，造成 14 人死亡，他们两人在同警方枪战中死亡。执法人员随后在他们的汽车上找到一部 iPhone 手机。

案发后不久，美国联邦调查局（Federal Bureau of Investigation, FBI）就带着搜查令找上门来，要求苹果公司提供关于这部手机的一切信息，库克给 FBI 的建议是：回去，给手机充上电，连上网络，让它自动备份，然后你们就能拿到数据。FBI 告诉苹果，他们已经重置了 iCloud 密码，备份需要输入新的 iCloud 密码，然而他们无法越过四位锁屏密码，所以，苹果提供的办法无法使用。FBI 随后要求苹果为其开发一套“政府系统”，在此系统下，他们可以对密码进行破解（四位密码只有一万种组合，破解起来并非难事，但正常情况下输错次数过多会导致手机停用）。

遭到苹果拒绝后，2016 年 2 月 16 日，FBI 亮出一份联邦法官的法庭指令，要求苹果为联邦调查局开发“政府系统”。随后，库克发内部信（公开信），回绝法院要求，表示自己的做法是在保护用户。2016 年 3 月 20 日，司法部宣布可能对苹果公司加密措施实施“旁路处理”，FBI 获得了来自某个第三方的可能的解锁方法，不需要苹果公司的调查协助，即可实现对嫌疑人的手机屏幕解锁并获取其中存储的数据。

在此案中，FBI 是根据一部 228 年前的《全令状法案》（All Writs Act, AWA）将苹果诉上法庭，该法案极其简短，最初仅包含两条：①最高法院和依照国会立法建立的所有法院，可以签发必要的或适当的令状以协助它们各自的司法管辖，该令状应符合惯例或法律原则；②享有管辖权的审判员或法官可以签发可选令状或规则令状。为了做出必要的限制，美国联邦法院在相关判例中，逐步建立了令状签发的限制规则，明确发行令状的特定情形，只有同时满足以下 4 个条件时，法院才能签发 AWA 令状：①缺失其他能够替代的救济方案；②独立的管辖权基础；③必要或适当的协助；④符合法律惯例和原则。

AWA 已经颁布 228 年，但直到 1977 年的 *United States v. New York Telephone Co.* 案中，才被用于刑事犯罪领域。这说明该法案是时代背景的产物，是美国稳固美国三权制衡的利器，最初并不被应用于协助执法，也不存在安全与隐私之争。但随着科技的快速发展与法律的迟延响应、公民隐私观念的深入、科技公司创新的需要、美国密码战争的影响、监控计划的不断曝光、恐怖主义的连续侵扰等因素，使得该法案浮出水面并且使用次数逐渐增加，直至圣伯纳迪诺市枪击案将争论推向高潮，倒逼美国国会和政府不得不重新进行审视，以找出更好的应对方案。

## 二、推特诉美国国土安全部案

2017 年 4 月 7 日，美国社交网站推特在旧金山联邦地区法院起诉美国国土安全部、美国海关和边境保护局以及这两个部门的 4 名工作人员，指责上述部门非法传唤，要求推特提供一位或多位推特用户身份信息，而这些推特用户多次发布了批评特朗普政府的言论。

根据推特提交的一份长达 25 页的起诉文件，美国国土安全部及旗下的美国海关和边境保护局要求推特交出一个叫@ALT\_USICIS 的账户背后运营者的身份信息，USICIS 是美国公民及移民服务局（U.S. Citizenship and Immigration Services）的简称，在推特上已有@USCIS 的官方账户，而创建于今年 1 月的@ALT\_USICIS，常常发布批评特朗普政府移民政策的推文。

@ALT\_USICIS 由几位号称是美国公民及移民服务局的前雇员进行运营，已经发表了 9 000 多条推文，多数为对特朗普政府的批评，该账户有近 4.6 万名粉丝。推特公司介绍说，在特朗普上任美国总统之后，推特上出现了一批特朗普政府的批评者，他们有的此前就在联邦政府不同部门工作，对政府工作有着独特的观察，并在推特上发表观点评论，持有与特朗普政府不同的意见。

这些批评者的账户名称通常相当“山寨”，常常会采用前缀或后缀加上政府机构缩写的形式来作为账户名称，用于发表对于该机构部门的批评言论，例如，一个专门批评美国劳工部（U.S. Department Labor）政策的账户就叫@alt\_labor，批评美国土地管理局（Federal Bureau of Land Management）的账户叫@blm\_alt，在推特上涌现了许多类似的账户，这些账户背后的运营者保持匿名，但相当活跃，



此次美国国土安全部盯上的@ALT\_USCIS 也是同类型账户之一。

2017 年 3 月 14 日，美国国土安全部下属的美国海关边境保护局对推特公司发出传唤，要求推特提供@ALT\_USCIS 运营者的身份信息。推特在诉讼文件中表示，当这些账户并没有被证明涉及违法犯罪时，政府要求获得账户的用户身份信息是违法的。“匿名且自由地发表对于公共事务的言论，这在美国政治生活中已是历史悠久的传统。”推特公司在诉讼文件中称，“美国宪法第一修正案包含了匿名自由发表关于公共事务言论的权利，由此赋予了推特用户言论自由的权利”<sup>①</sup>。

社交媒体推特于 2017 年 4 月 7 日撤销了其针对美国国土安全部的起诉，声称该政府机构已经取消了要求提供一个反特朗普总统的账户信息的传票。这家社交媒体的律师马克·弗拉纳根（Mark Flanagan）在写给法庭的一份文件中表示，美国司法部一位律师 4 月 7 日对推特说，该传票已经被取消并且索取反特朗普总统的账户信息的要求“不会再强行发生了”。

不过，美国国土安全部为何撤销传票以及它正在进行的相关调查是否已经结束，目前还未能立即弄清楚。对此，在法庭上为美国政府机构承担辩护工作的美国司法部拒绝置评，发出该传票的美国国土安全部也没有立即做出评论<sup>②</sup>。

以上两个案例可以看出，在崇尚自由与民主的美国，虽然协助执法制度已经相对完善，但是在执行过程中还是会遇到很多问题，国家安全和个人隐私的冲突最为明显。协助执法制度设立目的是预防犯罪和打击恐怖主义，维护社会公共秩序和国家安全，然而随着信息社会的发展和数据的电子化，个人信息更加脆弱和容易暴露。企业为了维护自身荣誉，赢得公众信任从而推动业务的持续发展，对个人隐私的保护也愈发重视，加上个人的隐私保护意识渐强，协助执法必然在实践中遇到重重困难。但出于国家安全或犯罪侦查需要，有时政府会强制进行协助执法，也获得了一些民众的理解和支持，在本节第三部分介绍对协助执法予以支持的两个案例。

### 三、其他相关案例

就 FBI 要求解锁的类似事件，若发生在佛罗里达州，则与发生在加利福尼亚

---

① 发表于 2017 年 4 月 7 日，链接为 <http://tech.163.com/17/0407/11/CHDRR3GE00097U7R.html>。

② 发表于 2017 年 4 月 8 日，链接为 <http://tech.163.com/17/0408/13/CHGLRT7000097U7R.html>。

州截然不同。在 2016 年 3 月 14 日举行的一个新闻发布会上，佛罗里达州波尔克县警长格雷迪·贾德（Grady Judd）讲述了他们破获的一个谋杀案。贾德称，犯罪嫌疑人利用智能手机拍摄了受害者的照片，不过后来给了警方智能手机的密码，以解锁他们的手机。当贾德被问及苹果拒绝帮助创建一个自定义固件，以允许 FBI “强行破解” 圣伯纳迪诺市枪击案查获的 iPhone 5C 时，他称：“你的商业模式不能是，‘我们不理睬联邦法官或州法官，我们凌驾于法律之上’。苹果首席执行官需要知道的是，他不能凌驾于法律之上，在美国任何人都不能。”他指出，如果他的部门未来碰到被锁定的 iPhone，可能导致库克被投入大牢，或许会依据蔑视法庭命令被指控。

2016 年 3 月 1 日，巴西联邦警方逮捕了 Facebook 拉美业务的副总裁 Diego Dzodan，原因是 Facebook 并未遵守一项旨在帮助调查人员侦查一桩毒品案的法庭命令，该案涉及一名 WhatsApp 用户。巴西联邦警方称，此次逮捕行动是应巴西东北部塞尔希培州（Sergipe）官员请求而实施的。联邦警方发表声明称，Facebook 及旗下通信应用 WhatsApp 屡次未遵守与一桩有组织罪案和非法毒品交易调查有关的法庭命令。鉴于该案的司法程序是秘密进行的，巴西警方并未提供此次抓捕行动的具体细节。针对该案，WhatsApp 和 Facebook 分别发表声明，WhatsApp 称，该公司对巴西警方的此次逮捕行动表示失望，并称其无法提供自己并不拥有的信息，这是由其服务的架构而决定的。声明表示：“我们在这桩案件中尽最大能力给予了配合。虽然我们尊重执法工作的重要性，但对其决定表示强烈的不认同。”Facebook 则指出，WhatsApp 独立于 Facebook 进行运营，这使得巴西警方逮捕 Facebook 高管显得“极端和不合适”<sup>①</sup>。

这两个案例表明，实践中也有一些政府对协助执法进行了大力支持，原因无外乎维护国家安全及侦查犯罪。从我国国内立法理念和制度考察：作为一个民主、文明的社会主义国家，我国立法积极保护个人权利和合法利益，但是当个人利益与国家利益发生冲突时，国家利益绝对高于个人利益，这是社会主义核心价值观的要素，也是宪法的基本精神。维护国家安全是协助执法法律制度的最高价值目标，是协助执法制度创制时首要考虑的要素。国家安全是整个社会赖

---

① 参考 <http://tech.sina.com.cn/i/2016-03-02/doc-ifxpvysx1813436.shtml>。

以存在的前提和基础，在恐怖袭击频发、网络犯罪严重的当下，国家安全和社会稳定更是每个公民和机构、组织尽全力维护的，协助执法制度是其应该履行的义务。

我国立法理念中始终强调在公权益和私权益发生冲突时，私权应当让位于公权，以执法为目的的活动不会产生过大的隐私保护争议。我国在《国家安全法》、《反恐怖主义法》和《网络安全法》等法律中均确立了明确的协助执法义务，包括协助解密义务（《反恐怖主义法》第十八条），而《宪法》第五条第五款规定：任何组织或者个人都不得有超越宪法和法律的特权。这意味着任何组织都必须遵守法律规定，协助执法机关的执法活动。

第四节 协助执法制度的法规遵从框架及建议

我国协助执法义务散见于 1995 年《人民警察法》、2000 年《电信条例》、2012 年《刑事诉讼法》，随着新技术和网络的普及使用，2015 年《国家安全法》、《反恐怖主义法》和 2016 年《网络安全法》对其进行了完善，增加了协助解密、数据留存的相关规定（见表 10-2）。

表 10-2 协助执法制度的法规遵从框架

法律名称	法律条款	法律规定
1995 年《人民警察法》	第十六条	公安机关因侦查犯罪的需要，根据国家有关规定，经过严格的批准手续，可以采取技术侦查措施
	第三十四条	人民警察依法执行职务，公民和组织应当给予支持和协助。公民和组织协助人民警察依法执行职务的行为受法律保护。对协助人民警察执行职务有显著成绩的，给予表彰和奖励
2000 年《电信条例》	第六十六条	电信用户依法使用电信的自由和通信秘密受法律保护。除因国家安全或者追查刑事犯罪的需要，由公安机关、国家安全机关或者人民检察院依照法律规定的程序对电信内容进行检查外，任何组织或者个人不得以任何理由对电信内容进行检查。 电信业务经营者及其工作人员不得擅自向他人提供电信用户使用电信网络所传输信息的内容

续表

法律名称	法律条款	法律规定
2012 年《刑事诉讼法》	第一百四十八条	<p>公安机关在立案后，对于危害国家安全犯罪、恐怖活动犯罪、黑社会性质的组织犯罪、重大毒品犯罪或者其他严重危害社会的犯罪案件，根据侦查犯罪的需要，经过严格的批准手续，可以采取技术侦查措施。</p> <p>人民检察院在立案后，对于重大的贪污、贿赂犯罪案件以及利用职权实施的严重侵犯公民人身权利的重大犯罪案件，根据侦查犯罪的需要，经过严格的批准手续，可以采取技术侦查措施，按照规定交有关机关执行。</p> <p>追捕被通缉或者批准、决定逮捕的在逃的犯罪嫌疑人、被告人，经过批准，可以采取追捕所必需的技术侦查措施</p>
	第一百四十九条	<p>批准决定应当根据侦查犯罪的需要，确定采取技术侦查措施的种类和适用对象。批准决定自签发之日起三个月以内有效。对于不需要继续采取技术侦查措施的，应当及时解除；对于复杂、疑难案件，期限届满仍有必要继续采取技术侦查措施的，经过批准，有效期可以延长，每次不得超过三个月</p>
	第一百五十条	<p>采取技术侦查措施，必须严格按照批准的措施种类、适用对象和期限执行。</p> <p>侦查人员对采取技术侦查措施过程中知悉的国家秘密、商业秘密和个人隐私，应当保密；对采取技术侦查措施获取的与案件无关的材料，必须及时销毁。</p> <p>采取技术侦查措施获取的材料，只能用于对犯罪的侦查、起诉和审判，不得用于其他用途。</p> <p>公安机关依法采取技术侦查措施，有关单位和个人应当配合，并对有关情况予以保密</p>
	第一百五十二条	<p>依照本节规定采取侦查措施收集的材料在刑事诉讼中可以作为证据使用。如果使用该证据可能危及有关人员的人身安全，或者可能产生其他严重后果的，应当采取不暴露有关人员身份、技术方法等保护措施，必要的时候，可以由审判人员在庭外对证据进行核实</p>
2015 年《国家安全法》	第四十二条	<p>国家安全机关、公安机关依法搜集涉及国家安全的情报信息，在国家安全工作中依法行使侦查、拘留、预审和执行逮捕以及法律规定的其他职权。</p> <p>有关军事机关在国家安全工作中依法行使相关职权</p>
	第七十七条	<p>公民和组织应当履行下列维护国家安全的义务：</p> <p>（一）遵守宪法、法律法规关于国家安全的有关规定；</p> <p>（二）及时报告危害国家安全活动的线索；</p> <p>（三）如实提供所知悉的涉及危害国家安全活动的证据；</p> <p>（四）为国家安全工作提供便利条件或者其他协助；</p> <p>（五）向国家安全机关、公安机关和有关军事机关提供必要的支持和协助；</p> <p>（六）保守所知悉的国家秘密；</p> <p>（七）法律、行政法规规定的其他义务。</p> <p>任何个人和组织不得有危害国家安全的行为，不得向危害国家安全的人或者组织提供任何资助或者协助</p>

续表

法律名称	法律条款	法律规定
2015 年《国家安全法》	第八十一条	公民和组织因支持、协助国家安全工作导致财产损失的，按照国家有关规定给予补偿；造成人身伤害或者死亡的，按照国家有关规定给予抚恤优待
2015 年《反恐怖主义法》	第十八条	电信业务经营者、互联网服务提供者应当为公安机关、国家安全机关依法进行防范、调查恐怖活动提供技术接口和解密等技术支持和协助
	第九十一条	拒不配合有关部门开展反恐怖主义安全防范、情报信息、调查、应对处置工作的，由主管部门处二千元以下罚款；造成严重后果的，处五日以上十五日以下拘留，可以并处一万元以下罚款。 单位有前款规定行为的，由主管部门处五万元以下罚款；造成严重后果的，处十万元以下罚款；并对其直接负责的主管人员和其他直接责任人员依照前款规定处罚
2016 年《网络安全法》	第二十一条	国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：（三）采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；（四）采取数据分类、重要数据备份和加密等措施
	第二十八条	网络运营者应当为公安机关、国家安全机关依法维护国家安全和侦查犯罪的活动提供技术支持和协助
	第五十九条	网络运营者不履行本法第二十一条、第二十五条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处一万元以上十万元以下罚款，对直接负责的主管人员处五千元以上五万元以下罚款
	第六十九条	网络运营者违反本法规定，有下列行为之一的，由有关主管部门责令改正；拒不改正或者情节严重的，处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员，处一万元以上十万元以下罚款：（三）拒不向公安机关、国家安全机关提供技术支持和协助的

综上所述可以看出，我国目前没有专门的协助执法法律，但在陆续颁布的新立法中不断对该制度进行了完善和调整。2015 年颁布的《反恐怖主义法》解决了长期以来未能解决的电信业务运营者、互联网服务提供者提供技术接口和解密等技术支持和协助的高位阶段的法律依据问题，同时也为《网络安全法》的“技术支持和协助”提供了内涵的背书。2016 年通过的《网络安全法》，使得公安机关、国家安全机关获得支持协助权的范围由信息提供扩展到了各类技术支持和协助（在实质上蕴含了信息提供、系统调用、接口提供、解密支持、人力协助等可能），同

时加大了网络运营者的法律责任。在具体适用方面，属于维护国家安全和侦查犯罪的情形，则适用《网络安全法》；属于防范、调查恐怖活动的情形，则适用《反恐怖主义法》。

值得注意的是，虽然《反恐怖主义法》和《网络安全法》顺应时代发展规定了协助解密义务、数据留存期限及相应的处罚制度，但没有详细的执行依据和标准，实践中会给企业遵从带来困难。关于协助执法的经济补偿规定更为简单，不具有强制执行力，与国外的财政拨款举措相比，容易显现执行乏力和义务主体消极守法的局面。这里的条款没有出现隐私保护的内容，这是法律制度的不足之处，我国没有专门的隐私或个人信息保护法，《网络安全法》中规定的数据保护内容是迄今为止最为全面的隐私保护制度，但没有关于合法拦截和数据留存过程中的数据访问限制，容易造成协助执法和隐私保护的割裂，扩大调查取证过程中隐私侵犯的潜在风险。信息化发达国家普遍制定了专门的通信协助执法制度：一般采取支持协助执法，同时合理限制其权力以降低个人干扰的立法方式，在协助执法义务中加入充分的隐私保护条款，尽量寻求平衡点，以此协调国家安全和个人隐私之间的冲突。

《国家安全法》规定的协助执法遵从的补偿，强调的是造成损害后的经济补偿，而不是对互联网服务提供者的守法成本补偿，前者发生在协助执法之后，而后者则发生在之前。因协助执法更偏重于加重企业成本，而鲜少直接对其造成经济损失，根据该法很难得到补偿，且实践中尚未出现类似案例。

## 第 11 章

# 个人信息保护

随着云计算、云存储、物联网等新技术的应用，人们通过社交网络、电子商务平台及移动智能终端等途径收集、处理的各种数据呈爆炸性增长，在容量、关系和复杂性等方面已超出了传统的处理能力和认知范畴，从而步入了大数据时代，

个人信息的保护问题因此而被提出新的挑战。纵观近年全球个人信息保护相关立法情况，正呈现出不断加强完善的趋势。个人信息与自然人切身利益紧密相关，与此同时，个人信息和数据安全已成为关系企业合并、分立、重组和上市审查的重要因素。个人信息控制者对个人信息的收集、处理、传输等行为，能够能动地影响个人利益、企业利益甚至国家利益。综上，个人信息保护问题在这个数据爆炸时代尤为敏感与突出，值得更多的关注与思考。

### 第一节 《网络安全法》相关规定及释义

我国《网络安全法》第四章“网络信息安全”对个人信息保护做出了明确的规定，以下将对相关条款的规定做出分析与解释。

《网络安全法》第四十条规定：网络运营者应当对其收集的用户信息严格保密，并建立健全用户信息保护制度。本条是关于网络运营者对用户信息保护制度的规

定。本条的约束主体为网络运营者，即网络的所有者、管理者和网络服务提供者。本条是对网络运营者保护用户信息义务的原则性规定，要求网络运营者对收集的用户信息严格保密，建立健全用户信息保护制度。其中用户包括自然人、法人和其他组织。因此本条规定的用户信息既包括个人信息和隐私，也包括法人和其他组织的商业秘密等信息。

第四十一条规定：网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。网络运营者不得收集与其提供的服务无关的个人信息，不得违反法律、行政法规的规定和双方的约定收集、使用个人信息，并应当依照法律、行政法规的规定和与用户的约定，处理其保存的个人信息。以上规定了合法、正当、必要原则与告知同意规则。合法正当原则之合法性，即收集、使用个人信息相关行为应当符合现有法律法规要求，如经过权利人同意、履行法定义务，为提供服务而与第三方签订的协议，但该协议不得从事损害权利人的利益，且应严格遵循安全保障措施要求；正当性，即个人信息相关行为应当具备正当理由，如为服务之目的，履行职责之目的，为权利人之利益，为公共利益等，不应超出处理前所确定告知用户的目的；必要性，即个人信息相关行为应以应确保为前述目的实现之必须。确保无过多处理，无不相关个人信息，不需要时及时删除等。告知同意规则要求个人信息的收集、处理、传输、披露等行为应提前告知个人信息主体，包括相关行为的目的、方式、范围、后果、救济途径，主体参与途径，同意的撤回途径，个人信息的保护措施等关切个人信息主体利益的因素。其中后果包括同意与不同意的两个方面。告知同意机制的价值在于充分尊重用户的知情权和选择权。然而，随着技术进步与发展，个人信息收集处理场景日益丰富多样，对告知同意机制的有效性带来挑战。告知同意作为个人信息处理的重要因素已被认为难以满足用户的知情权、选择权。特别是通过产品、服务使用用户协议默认勾选的方式，加之用户行为惯性导致用户并未真正知晓其个人信息被收集、使用的情况如何，甚至“如不同意本协议则请不要使用本产品或服务”的格式条款使得用户并无实质的选择权，告知同意机制在此情况下难以发挥保障用户知情选择权的作用。

第四十二条规定：网络运营者不得泄露、篡改、毁损其收集的个人信息；未



经被收集者同意，不得向他人提供个人信息。但是，经过处理无法识别特定个人且不能复原的除外。网络运营者应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失。在发生或者可能发生个人信息泄露、毁损、丢失的情况时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。本条是关于个人信息安全原则、个人信息的匿名化处理规则及个人信息泄露的补救和报告义务。个人信息安全原则是个人信息保护的一项重要原则，是指个人信息应该处于适当的安全保护之中，避免遭受未经授权的获取、破坏、使用、修改和披露。个人信息安全原则包括两个层面的意思，一是要求网络运营者不得泄露、篡改、毁损其收集的个人信息；二是要求网络运营者采取必要的措施，包括物理的、技术的及管理的措施以确保个人信息不被泄露、毁损和丢失。个人信息的匿名化，是指移除信息中可以识别个人信息的部分，并通过特定的方法，使得信息主体不会被识别出来。个人信息的泄露补救和报告义务，是指在发生或者可能发生个人信息泄露、毁损、丢失的情况时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。但是对于哪些情形需要向用户告知，向有关部门报告，以及在什么期限、采取什么方式向用户告知、向有关部门报告，需要根据不同的情况做出具体的规定。

第四十三条规定：个人发现网络运营者违反法律、行政法规的规定或者双方的约定收集、使用其个人信息的，有权要求网络运营者删除其个人信息；发现网络运营者收集、存储的其个人信息有错误的，有权要求网络运营者予以更正。网络运营者应当采取措施予以删除或者更正。本条是关于个人信息的删除权与更正权的规定。个人信息的删除权，是指信息主体在具备法定的理由的情况下请求删除其个人信息的权利。个人在以下情况下可以行使其信息的删除请求权：一是收集、使用行为不具备合法性。例如，收集、使用开始时就未得到被收集者的同意且无法律依据，被收集者的同意无效或已被撤销，对收集、使用信息超出法定或者约定的范围的。二是收集、使用个人信息的目的消失，使对个人信息的保护及处理、利用失去了必要性、正当性。三是约定的收集、使用、保存个人信息的期限届满。对删除个人信息的要求，网络运营者应当及时受理并采取措施予以删除；个人信息的更正权，是指在个人信息收集、存储、使用过程中，个人信息不完整或者不准确时，个人有权要求及时更正、补充的权利。本条赋予了信息主体对其

信息的更正权，有权要求网络运营者更正和补充其个人信息的错误和遗漏。对更正个人信息的要求，网络运营者应当及时受理并采取措施予以更正。

第四十四条规定：任何个人和组织不得窃取或者以其他非法方式获取个人信息，不得非法出售或者非法向他人提供个人信息。本条规定了两个层面的内涵：一是个人和组织不得非法获取个人信息。本条的义务主体既包括个人，也包括组织。所谓非法获取是指未经收集者同意，以非法方式取得被收集者的个人信息。二是不得非法出售、提供个人信息。根据第四十二条的规定，在个人同意的前提下才能向其他人提供个人信息。向他人提供包括通过出售、共享、公开等方式将个人信息提供给他人，都构成非法出售、非法提供个人信息的行为。

第四十五条规定：依法负有网络安全监督管理职责的部门及其工作人员，必须对在履行职责中知悉的个人信息、隐私和商业秘密严格保密，不得泄露、出售或者非法向他人提供。本条是关于负有网络安全监督管理职责的部门及其工作人员的保密义务的规定。个人信息的保护主体除网络产品、服务的提供者，网络运营者外，依法负有网络安全监督管理职责的部门及其工作人员也要严格保密其在履行职责过程中知悉的个人信息，不得泄露、出售或者非法向他人提供。

## 第二节 个人信息保护制度概述

### 一、个人信息相关概念释义

“可识别性”是个人信息的重要属性，依据个人信息保护原理，能够直接或间接识别自然人个人身份的信息均为个人信息。2017年6月1日实施的《网络安全法》第七十六条第五款规定：个人信息，是指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》对“公民个人信息”的定义也体现识别性的本质，并以信息的重要程

度作为量刑的重要依据。个人信息相关的行为通常包括收集、处理、传输、对外提供、删除等，其中个人信息收集是指为特定目的而取得权利人个人信息的行为，收集行为是提供服务、对个人信息进行再利用的前提。关于个人信息处理行为的界定，从狭义角度进行解读，即个人信息处理行为仅指个人信息控制者或个人信息代处理者对其控制范围内的个人信息所进行的存储、加工、使用、披露、分析利用行为。依据《关键信息安全术语》，传输，是指通过电子方式将信息从某一点发送至另一点或其他多个点的状态，包括通过网页、软件进行的传输、通过物理电子介质等方式进行的传输。对外提供，是指个人信息相关主体将个人信息提供给独立的第三方的行为。删除，即对个人信息所进行的删除操作，依据权利主体要求或法规要求，个人信息控制者应及时删除其存储的个人信息。

由于不同的法律传统及使用习惯，各国在个人信息保护立法中使用的基本概念也不尽相同，总体来说有三个，分别为“个人信息”、“隐私”与“个人数据”。其中，使用“个人数据”概念的国家或地区最多，主要集中在欧盟、欧盟成员及受欧盟 1995 年数据保护指令立法影响的其他国家。在普通法国家（英国除外），如美国、澳大利亚、新西兰、加拿大及受美国影响较大的 APEC 的成员等，则大多使用隐私概念。日本、韩国及俄罗斯等国则使用“个人信息”概念。从我国立法表述来看，更倾向于采用“个人信息”的表述。

## 二、大数据背景下对“个人信息”的重新审视

“可识别性”是个人信息的重要属性，但区分可识别性程度的工具是技术。数据收集与再识别化<sup>①</sup>技术的应用使得越来越多的个人价值密度低的原始数据更易被赋予“可识别性”特征。例如，商业机构通过有效组合和集成互联网用户的消费信息、网页收集信息、社交网络上的个人信息、智能手机的位置信息以及智能电表等揭示出的消费习惯信息等，就可快速对某特定的自然人“塑形”。以智能电表的使用为例，一般意义上电表所记录的用电数据并不属于个人信息，但是随着智能电表的普及数据再识别化技术的发展，智能电表所产生的个人用电数据也可

---

<sup>①</sup> 数据的再识别化是指通过大量集合数据（而不是抽样而得来的数据或因果关系的数据）应用非公开的运算法则，分析不同的数据之间的相关性，相关机构可以探索或者推测之前不知道的事实和模式。

能成为个人信息的范畴<sup>①</sup>。不难预知，大数据的发展，以及相关技术的应用将使得传统上不可识别的一些数据转化为可识别的数据，从而拓宽个人信息的范围。

### 三、大数据背景下欧美个人信息保护立法趋势

权利保障与信息自由流动的“恰当平衡”是一个抽象的意念，如何在尊重各国文化、法律、政治及经济发展实际状况的基础上，将其内化到个人信息保护法律规则的制定中是最大的难题，也是世界各国、各地区个人信息保护立法最主要的分歧所在。欧盟个人信息保护立法是世界上最先进，也最为严苛的，从“个人数据保护指令”到“一般数据保护条例”的变革，无不体现着欧盟将个人信息权利保护作为终极价值追求。美国是信息技术发展的领头羊，个人信息保护立法更倾斜于对信息自由流动的关切。梳理和分析欧盟个人信息保护立法的动向与趋势对促进我国个人信息保护立法意义重大。

#### （一）欧盟个人信息保护立法制度

近年来，欧盟个人信息保护立法改革的持续推进成为信息时代的一大盛事，牵动着全世界的目光。欧盟个人信息保护立法改革是“内忧”和“外患”共同作用的结果。大数据、云计算以及数据挖掘与分析技术的快速发展使制定于 20 年前的《个人数据保护指令》（全称为“1995 年 10 月 24 日欧洲议会与欧盟理事会关于个人信息处理中个人权利保护及促进数据自由流通的第 95/46/EC 号指令”，Directive 95/46/EC of the European Parliament of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data，以下简称《指令》）难以有力应对个人信息被非法窃取、破坏和监控的难题，将于 2018 年生效的《一般数据保护条例》<sup>②</sup>（General Data

① 在智能电表的使用中，个人生活用电时每种电器在工作和通电情况下的负荷特征是不同的，而智能电表能够持续地详细记录这些特征，并将收集和存储，对这些用电数据的分析，可以知道人们在某一时间段所打开的电器以及进行的活动，进而可以利用长期积累的数据推测人们的日常生活习惯，如作息时间，而这些显然已经可以归属于个人信息的范畴。

② 2016 年 4 月 14 日，欧洲议会投票通过了商讨四年的《一般数据保护条例》（General Data Protection Regulation），该条例将在欧盟官方杂志公布正式文本的两年后（2018 年）生效。新条例的通过意味着欧盟对个人信息保护及其监管达到了前所未有的高度，堪称史上最严格的数据保护条例。新条例将取代 1995 年发布的《欧盟数据保护指令》（Directive 95/46/EC），并直接适用于欧盟各成员。

Protection Regulation, GDPR, 以下简称《条例》)在这一背景下应运而生。另外,“棱镜门”丑闻使欧—美在数据跨境流动与数据保护双边合作中的信任度降至冰点。为应对“外患”,欧盟加速推进个人信息保护立法改革的步伐,积极与美国展开磋商与合作,以期重建欧—美数据流通的信任机制。总之,欧盟数据保护立法呈现以下发展趋势。

### 1. 提升立法的统一性

为改善和消除《指令》在实施中的“不确定性”与“不一致性”,欧盟从数据保护立法与执法的两个主要环节入手,通过改革既有规则和创设新规则,旨在提升数据保护立法的统一性与执法一致性、高效性。

根据《欧洲联盟运作条约》(Treaty on the Functioning of the European Union, TFEU)第 288 条之规定,“指令”针对每个成员而不是当事人,成员有权选择具体的形式、方法制定国内法以执行指令,而“条例”生效即成为国内法的一部分,无论是对于成员还是当事人都具有广泛的约束力。欧盟将个人信息保护立法从“指令”提升至“条例”,以确保“一个欧洲一部数据保护法”,这一改革事项在欧洲议会与欧盟理事会层面取得基本共识。较之《指令》,《条例》在生效后将带来更高层次上的统一适用,特别是一些成员分歧较大的核心法律概念与规则的统一定义<sup>①</sup>将有效降低法律“不确定”的负面影响。

### 2. 强化个人信息权利的保护力度

保护个人信息权利在欧盟被视为公民的一项宪法性权利。新技术带来的挑战使欧盟认识到个人信息保护的紧迫性。欧盟将强化数据主体的权利保护作为数据保护立法改革的最重要的政策目标之一,其实现方式具体如下。

#### ● 深化个人信息保护的透明度原则

透明度原则是欧盟数据保护立法的基本原则。提升个人数据保护的透明度是增强数据主体个人信息控制力,保护个人信息权利的基本途径之一。《条例》进一步深化了该原则,第十二条规定:数据控制者应对个人信息处理和数据主体权利行使实施透明度和便利访问的策略。数据控制者应该以浅显易懂的形式,运用朴素的语言向数据主体提供关于个人信息处理的交流及信息,特别是涉及儿童的信

<sup>①</sup> 例如,“个人信息”、“敏感个人信息”、“通知—同意”、“充分性”保护等。

息。第十四条规定：当数据主体的个人信息被收集时，至少应告诉数据主体数据控制者的身份、联系方式、控制者的代理人及数据保护专员；数据的处理目的；存储期限；数据主体享有访问、更改、删除或拒绝处理的权利；向监管机构提起申诉的权利等。透明度原则的深化使数据主体清楚地判断所做出的积极同意是否有必要，这种有效性判断可防止数据控制者依据个人信息而产生的用户歧视，并促进个人信息在保存与使用中的问责机制的建立<sup>①</sup>。

- 提升了对数据主体“赋权”的力度

一是引入数据主体的“积极同意”规则，以强化数据主体对个人信息的控制能力。《指令》并未明确个人“同意”是“积极同意”还是“消极同意”，而欧盟委员会在《条例》中引入了“积极同意（Explicit Consent）”规则。第四条规定，数据主体“同意”是指数据主体依照其意愿自愿做出的任何指定的、具体的、知情的及明确的指示。通过声明或明确肯定的行为做出的这种指示，意味着其同意与他有关的个人数据被处理。第七条规定，数据主体还有权在任何时候撤回同意。《条例提案》第十七条规定了数据被遗忘权，即在法律限定条件下，数据主体有权要求数据控制者立即删除其直接控制的个人信息。当被要求删除的个人信息已经被数据控制者公开时，则数据主体有权要求数据控制者采取一切合理措施（包括技术措施），通知处理个人信息的第三方按照数据主体的要求删除个人信息的链接、副本或复印件。随后，在欧盟理事会还未就此达成一致意见时，欧盟最高法院已在“谷歌西班牙案”中通过“不可上诉判决”的形式对数据遗忘权加以确认。被遗忘权的提出增加了数据主体对个人信息的控制能力，也符合了大数据时代人们对个人隐私保护的强烈需求。但数据遗忘权的提出在欧盟引发了巨大争议，言论自由、数字经济发展、科研进步与国家安全成为反对者对该权利攻击的矛头。

## （二）美国个人信息保护立法制度

在大数据背景下，美国也在积极推动相关立法与政策变革，以期回应大数据发展对隐私保护带来的挑战。2012年美国奥巴马签署美国白宫发布的工作报

---

① ARTEMI RALLO. International Standard on the Protection of Personal data and privacy: The Madridre solution [EB/OL]. [2017-8-15] [http://www.privacy\\_conference2009.org/dpas\\_space/space\\_reserved/documentos\\_adaptados/common/2009\\_Madrid/estandares\\_resolucion\\_madrid\\_en.pdf](http://www.privacy_conference2009.org/dpas_space/space_reserved/documentos_adaptados/common/2009_Madrid/estandares_resolucion_madrid_en.pdf).

告《网络环境下消费者数据的隐私保护——在全球数字经济背景下保护隐私和促进创新的政策框架》（简称《隐私权报告》），《消费者隐私权利法案》（Consumer Privacy Bill of Rights, CPBR）随之被提出。该法案对于消费者隐私保护标注做出明确规定，包括个人控制、透明性、相关环境、可修改和准确性、聚焦收集、问责<sup>①</sup>。2014 年，美国总统执行办公室发布全球大数据“白皮书”——《大数据：把握机遇，守护价值》<sup>②</sup>。“白皮书”对于美国大数据应用与管理现状、政策框架和改进建议做出了集中阐述。对于大数据发展与隐私保护的问题上，“白皮书”提到“在许多情况下，告知与同意仍是隐私保护的一种基本模式存在，但如今，我们需要做出判断，在大数据环境下，更侧重于数据的使用和重复使用的研究方式是否会成为使隐私权管理更为高效的基础。或许，建立一种使个体参与从其个人信息采集后的使用和分配问题的机制，将是更好的授权方法，以使人们能够从其个人信息中获利。隐私保护的方式也必须不断发展，以适应大数据所带来的社会效益”。2017 年 3 月，美国参、众两院先后宣布废除联邦通信委员会于 2016 年 10 月颁布的网络用户隐私保护规则，这不仅激化了美国国内的互联网公司与消费者的对立，更会导致美欧个人信息保护战的进一步升级。综上，美国政府对个人信息保护的基本思路仍然是在鼓励大数据发展的前提下，以解决问题的思路应对隐私保护问题。这也集中体现了美国在平衡技术进步与个人信息保护关系中的基本价值取向——对技术进步与经济发展更为关切。

### 第三节 典型案例

随着网络安全法及个人信息保护的相关法规及司法解释的出台与实施，个人信息保护的司法与执法得到社会的关注。最高人民法院、最高人民检察院（以下简称

① 个人控制：消费者可以对企业从自己这里收集什么信息，以及如何使用这些信息进行控制；透明：消费者有权简单易懂地获取有关隐私权与安全实践的信息；相关环境：消费者有权得知企业如何在消费者提供信息的相关环境方面进行收集、使用与披露用户数据安全：消费者的个人信息必须得到安全与负责任地处理；可修改和准确性：因个人信息的敏感性，以及不准确的数据会对消费者有产生不良后果的风险，消费者有权查阅并更正个人资料；聚焦收集：企业在合理的限度内收集与保存用户数据；问责：拥有个人信息的公司有义务采取适当措施，以确保它们符合《消费者隐私权法案》，参考 <http://www.alibuybuy.com/posts/85030.html>。

② 参考 <http://www.199it.com/archives/233121.html>。

“两高”)均公开侵犯公民个人信息犯罪典型案例,以下以其中两个案例展开论述。

## 一、韩世杰、旷源鸿、韩文华等侵犯公民个人信息案,非法查询征信信息牟利,构成侵犯公民个人信息罪

### (一) 基本案情

2015年9月3日至4日,被告人韩世杰、旷源鸿、韩文华利用连光辉(湖北省巴东县农村商业银行沿渡河支行征信查询员)的征信查询ID号、密码及被告人李冲、耿健美(洛阳银行郑州东风路支行客户经理)提供的洛阳银行郑州东风路支行的银行专用网络,在该行附近使用计算机非法查询公民个人银行征信信息3万余条。

2015年9月5日至6日,被告人韩世杰、旷源鸿、韩文华利用连光辉的征信查询ID号、密码及被告人李楠、卢惠生(德州银行滨州金廷支行行长)提供的德州银行滨州分行的银行专用网络,在该行南面的停车场内,使用计算机分两次非法查询公民个人银行征信信息2万余条。

2015年9月8日,被告人韩世杰、旷源鸿、韩文华利用李涛(江苏省淮安市农村商业银行徐溜支行职工)的银行征信查询ID号及密码及被告人李楠、卢惠生提供的德州银行滨州分行专用网络,在该行南面的停车场内,使用计算机非法查询公民个人银行征信信息近3万条。

被告人韩亮、邓佳勇获得征信查询ID号、密码并非法提供给被告人韩世杰等人使用,双方通过被告人陈莎莎中转租金、传递密码。被告人韩世杰、旷源鸿、韩文华将查询获得的上述公民个人银行征信信息出售给他人,向被告人韩亮、李冲、李楠支付了相关费用。

### (二) 裁判结果

湖北省巴东县人民法院判决认为:被告人韩世杰、旷源鸿、韩文华、韩亮、邓佳勇、李楠、陈莎莎、卢惠生、李冲、耿健美违反国家有关规定,非法获取公民个人信息出售牟利,情节严重,其行为已构成侵犯公民个人信息罪。综合考虑



被告人自首、坦白、积极退赃等情节，以侵犯公民个人信息罪判处被告人韩世杰有期徒刑一年六个月，并处罚金人民币二万元；被告人旷源鸿有期徒刑一年三个月，并处罚金人民币二万元；被告人韩文华判处有期徒刑一年二个月，并处罚金人民币一万元；被告人韩亮有期徒刑一年，并处罚金人民币一万元；以及其他各被告人相应有期徒刑、拘役和罚金。该判决已发生法律效力。

### （三）典型意义

依据《网络安全法》、《刑法》二百五十三条，两高《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》将在履行职责或者提供服务过程中获得的公民个人信息出售或者提供给他人的入罪标准减半，且明确规定从重处罚。通过降低入罪标准与从重处罚，能够起到预防与教育作用。对于网络运营者、网络服务提供者而言，应当健全内部管理制度、严格规范员工行为，并做好员工培训工作。

## 二、肖凡、周浩等侵犯公民个人信息案，利用黑客手段窃取公民个人信息出售牟利，构成侵犯公民个人信息罪

### （一）基本案情

被告人肖凡、周浩预谋窃取邮局内部的公民个人信息进行出售牟利，共同出资购买了黑客软件。2016 年 5 月至 2016 年 6 月，两人通过黑客软件侵入邮局内网，在邮局内网窃取邮局内部的公民个人信息 103 257 条，并将窃取的公民个人信息全部出售给被告人李晓波。后李晓波将购买的公民个人信息出售给被告人王丽元 40 000 条，王丽元又将购买到的公民个人信息出售给被告人宋晓波 30 000 条。

### （二）裁判结果

内蒙古自治区赤峰市红山区人民法院判决认为：被告人肖凡、周浩通过黑客手段窃取公民个人信息并非法出售，李晓波、王丽元、宋晓波通过购买方式非法获取公民个人信息，其行为均已构成侵犯公民个人信息罪。据此，以侵犯公民个

人信息罪判处被告人肖凡、周浩、李晓波各有期徒刑两年，并处罚金人民币五万元；被告人王丽元有期徒刑一年，并处罚金人民币三万元；被告人宋晓波有期徒刑六个月，并处罚金人民币三万元。该判决已发生法律效力。

### （三）典型意义

利用黑客工具侵入计算机信息系统窃取个人信息并出售，同时触犯两个罪名即非法侵入计算机信息系统罪与侵犯公民个人信息罪，两罪均有单位犯罪。《网络安全法》第二十七条将非法侵入他人网络、窃取网络数据等行为定位为危害网络安全的行为并在第六十三条规定了行政处罚措施，同时对受过治安处罚或刑事处罚的人员进行了从业限制或禁止性规定。无论利用黑客工具或为他人提供黑客工具非法入侵计算机信息系统、获取个人信息及其他数据均为法律法规所禁止。

## 第四节 个人信息保护的法规遵从框架及建议

在个人信息保护层面，我国已经出台了不同位阶的法律法规以规制个人信息滥用行为，包括《民法总则》第一百一十一条，《刑法修正案（七）（九）》第十七条、第二十八条，《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》，《最高人民法院关于审理利用信息网络侵害人身权益民事纠纷案件适用法律若干问题的规定》，《中华人民共和国反恐怖主义法》（以下简称《反恐怖主义法》），《中华人民共和国消费者权益保护法》（以下简称《消费者权益保护法》）第十四条、第二十九条、第五十条、第五十六条，《中华人民共和国居民身份证法》（以下简称《居民身份证法》，2011年修订），《电信和互联网用户个人信息保护规定》，《互联网用户账号名称管理规定》，《通信短信息服务管理规定》，《寄送服务用户个人信息安全管理规范》，《中华人民共和国测绘法》（以下简称《测绘法》，2017年修订），《中国人民银行关于银行金融机构做好个人金融信息保护工作的通知》，《中国人民银行关于今日评机构进一步做好客户个人金融信息保护工作的通知》，《征信业管理条例》，《网络预约出租汽车经营服务管理暂行办法》，《规范互联网信息服务市场秩序若干规定》，《中华人民共和国旅游法》（以下简称《旅游法》，2016年修订），第五十二

条《电子商务法（草案）》等近二十项相关法律法规。以下将对上述法律法规遵从框架做出列举。

## 一、我国个人信息保护的法规遵从框架

我国个人信息保护的法规遵从框架如表 11-1 所示。

表 11-1 我国个人信息保护的法规遵从框架

法律名称	具体规定	发布机构及生效时间	法律状态
《民法总则》	第一百一十一条 自然人的个人信息受法律保护。任何组织和个人需要获取他人个人信息的，应当依法取得并确保信息安全，不得非法收集、使用、加工、传输他人个人信息，不得非法买卖、提供或者公开他人个人信息	全国人大常委会， 2017-10-1	已发布， 未生效
《中华人民共和国侵权责任法》 （以下简称《侵权责任法》）	第二条 侵害民事权益，应当依照本法承担侵权责任。本法所称民事权益，包括生命权、健康权、姓名权、名誉权、荣誉权、肖像权、隐私权、婚姻自主权、监护权、所有权、用益物权、担保物权、著作权、专利权、商标专用权、发现权、股权、继承权等人身、财产权益	全国人大常委会， 2010-7-1	现行有效
《刑法修正案》	第十七条 将刑法第二百五十三条之一修改为“违反国家有关规定，向他人出售或者提供公民个人信息，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。违反国家有关规定，将在履行职责或者提供服务过程中获得的公民个人信息，出售或者提供给他人的，依照前款的规定从重处罚。窃取或者以其他方法非法获取公民个人信息的，依照第一款的规定处罚。单位犯前三款罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，依照各该款的规定处罚。” 第二十八条 在刑法第二百八十六条后增加一条，作为第二百八十六条之一：“网络服务提供者不履行法律、行政法规规定的信息网络安全管理义务，经监管部门责令采取改正措施而拒不改正，有下列情形之一的，处三年以下有期徒刑、拘役或者管制，并处或者单处罚金：（一）致使违法信息大量传播的；（二）致使用户信息泄露，造成严重后果的；（三）致使刑事案件证据灭失，情节严重的；（四）有其他严重情节的。单位犯前款罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，依照前款的规定处罚。有前两款行为，同时构成其他犯罪的，依照处罚较重的规定定罪处罚”	全国人大常委会， 2015-11-1	现行有效

续表

法律名称	具体规定	发布机构及生效时间	法律状态
《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》	<p>第一条 刑法第二百五十三条之一规定的“公民个人信息”，是指以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息，包括姓名、身份证件号码、通信通讯联系方式、住址、账号密码、财产状况、行踪轨迹等。</p> <p>第二条 违反法律、行政法规、部门规章有关公民个人信息保护的规定的，应当认定为刑法第二百五十三条之一规定的“违反国家有关规定”。</p> <p>第三条 向特定人提供公民个人信息，以及通过信息网络或者其他途径发布公民个人信息的，应当认定为刑法第二百五十三条之一规定的“提供公民个人信息”。未经被收集者同意，将合法收集的公民个人信息向他人提供的，属于刑法第二百五十三条之一规定的“提供公民个人信息”，但是经过处理无法识别特定个人且不能复原的除外。</p> <p>第四条 违反国家有关规定，通过购买、收受、交换等方式获取公民个人信息，或者在履行职责、提供服务过程中收集公民个人信息的，属于刑法第二百五十三条之一第三款规定的“以其他方法非法获取公民个人信息”。</p> <p>第五条 非法获取、出售或者提供公民个人信息，具有下列情形之一的，应当认定为刑法第二百五十三条之一规定的“情节严重”：</p> <p>（一）出售或者提供行踪轨迹信息，被他人用于犯罪的；</p> <p>（二）知道或者应当知道他人利用公民个人信息实施犯罪，向其出售或者提供的；</p> <p>（三）非法获取、出售或者提供行踪轨迹信息、通信内容、征信信息、财产信息五十条以上的；</p> <p>（四）非法获取、出售或者提供住宿信息、通信记录、健康生理信息、交易信息等其他可能影响人身、财产安全的公民个人信息五百条以上的；</p> <p>（五）非法获取、出售或者提供第三项、第四项规定以外的公民个人信息五千条以上的；</p> <p>（六）数量未达到第三项至第五项规定标准，但是按相应比例合计达到有关数量标准的；</p> <p>（七）违法所得五千元以上的；</p> <p>（八）将在履行职责或者提供服务过程中获得的公民个人信息出售或者提供给他人，数量或者数额达到第三项至第七项规定标准一半以上的；</p> <p>（九）曾因侵犯公民个人信息受过刑事处罚或者两年内受过行政处罚，又非法获取、出售或者提供公民个人信息的；</p>	最高人民法院、最高人民检察院，2017-6-1	现行有效

续表

法律名称	具体规定	发布机构及生效时间	法律状态
《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》	<p>(十) 其他情节严重的情形。实施前款规定的行为, 具有下列情形之一的, 应当认定为刑法第二百五十三条之一第一款规定的“情节特别严重”: (一) 造成被害人死亡、重伤、精神失常或者被绑架等严重后果的; (二) 造成重大经济损失或者恶劣社会影响的; (三) 数量或者数额达到前款第三项至第八项规定标准十倍以上的; (四) 其他情节特别严重的情形。</p> <p>第六条 为合法经营活动而非法购买、收受本解释第五条第一款第三项、第四项规定以外的公民个人信息, 具有下列情形之一的, 应当认定为刑法第二百五十三条之一规定的“情节严重”: (一) 利用非法购买、收受的公民个人信息获利五万元以上的; (二) 曾因侵犯公民个人信息受过刑事处罚或者两年内受过行政处罚, 又非法购买、收受公民个人信息的; (三) 其他情节严重的情形。实施前款规定的行为, 将购买、收受的公民个人信息非法出售或者提供的, 定罪量刑标准适用本解释第五条的规定。</p> <p>第七条 单位犯刑法第二百五十三条之一规定之罪的, 依照本解释规定的相应自然人犯罪的定罪量刑标准, 对直接负责的主管人员和其他直接责任人员定罪处罚, 并对单位判处罚金。</p> <p>第八条 设立用于实施非法获取、出售或者提供公民个人信息违法犯罪活动的网站、通讯群组, 情节严重的, 应当依照刑法第二百八十七条之一的规定, 以非法利用信息网络罪定罪处罚; 同时构成侵犯公民个人信息罪的, 依照侵犯公民个人信息罪定罪处罚。</p> <p>第九条 网络服务提供者拒不履行法律、行政法规规定的信息网络安全管理义务, 经监管部门责令采取改正措施而拒不改正, 致使用户的公民个人信息泄露, 造成严重后果的, 应当依照刑法第二百八十六条之一的规定, 以拒不履行信息网络安全管理义务罪定罪处罚。</p> <p>第十条 实施侵犯公民个人信息犯罪, 不属于“情节特别严重”, 行为人系初犯, 全部退赃, 并确有悔罪表现的, 可以认定为情节轻微, 不起诉或者免于刑事处罚; 确有必要判处刑罚的, 应当从宽处罚。</p>	最高人民法院、最高人民检察院, 2017-6-1	现行有效

续表

法律名称	具体规定	发布机构及生效时间	法律状态
《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》	<p>第十一条 非法获取公民个人信息后又出售或者提供的，公民个人信息的条数不重复计算。向不同单位或者个人分别出售、提供同一公民个人信息的，公民个人信息的条数累计计算。对批量公民个人信息的条数，根据查获的数量直接认定，但是有证据证明信息不真实或者重复的除外。</p> <p>第十二条 对于侵犯公民个人信息犯罪，应当综合考虑犯罪的危害程度、犯罪的违法所得数额以及被告人的前科情况、认罪悔罪态度等，依法判处有期徒刑。罚金数额一般在违法所得的一倍以上五倍以下</p>	最高人民法院、最高人民检察院，2017-6-1	现行有效
《最高人民法院关于审理利用信息网络侵害人身权益民事纠纷案件适用法律若干问题的规定》	<p>第十二条 网络用户或者网络服务提供者利用网络公开自然人基因信息、病历资料、健康检查资料、犯罪记录、家庭住址、私人活动等个人隐私和其他个人信息，造成他人损害，被侵权人请求其承担侵权责任的，人民法院应予支持。但下列情形除外：（一）经自然人书面同意且在约定范围内公开；（二）为促进社会公共利益且在必要范围内；（三）学校、科研机构等基于公共利益为学术研究或者统计的目的，经自然人书面同意，且公开的方式不足以识别特定自然人；（四）自然人自行在网络上公开的信息或者其他已合法公开的个人信息；（五）以合法渠道获取的个人信息；（六）法律或者行政法规另有规定。网络用户或者网络服务提供者以违反社会公共利益、社会公德的方式公开前款第四项、第五项规定的个人信息，或者公开该信息侵害权利人值得保护的重大利益，权利人请求网络用户或者网络服务提供者承担侵权责任的，人民法院应予支持。国家机关行使职权公开个人信息的，不适用本条规定</p>	最高人民法院，2014-10-10	现行有效
《反恐怖主义法》	<p>第四十八条 反恐怖主义工作领导小组机构、有关部门和单位、个人应当对履行反恐怖主义工作职责、义务过程中知悉的国家秘密、商业秘密和个人隐私予以保密。违反规定泄露国家秘密、商业秘密和个人隐私的，依法追究法律责任</p>	全国人大常委会，2016-1-1	现行有效
《消费者权益保护法》	<p>第十四条 消费者在购买、使用商品和接受服务时，享有人格尊严、民族风俗习惯得到尊重的权利，享有个人信息依法得到保护的权利。</p>	全国人大常委会，2014-3-15	现行有效

续表

法律名称	具体规定	发布机构及生效时间	法律状态
《消费者权益保护法》	<p>第二十九条 经营者收集、使用消费者个人信息，应当遵循合法、正当、必要的原则，明示收集、使用信息的目的、方式和范围，并经消费者同意。经营者收集、使用消费者个人信息，应当公开其收集、使用规则，不得违反法律、法规的规定和双方的约定收集、使用信息。</p> <p>第五十条 经营者侵害消费者的人格尊严、侵犯消费者人身自由或者侵害消费者个人信息依法得到保护的权利的，应当停止侵害、恢复名誉、消除影响、赔礼道歉，并赔偿损失。</p> <p>第五十六条 经营者有下列情形之一的，除承担相应的民事责任外，其他有关法律、法规对处罚机关和处罚方式有规定的，依照法律、法规的规定执行；法律、法规未作规定的，由工商行政管理部门或者其他有关行政部门责令改正，可以根据情节单处或者并处警告、没收违法所得、处以违法所得一倍以上十倍以下的罚款，没有违法所得的，处以五十万元以下的罚款；情节严重的，责令停业整顿、吊销营业执照：……（九）侵害消费者人格尊严、侵犯消费者人身自由或者侵害消费者个人信息依法得到保护的权利的……经营者有前款规定情形的，除依照法律、法规规定予以处罚外，处罚机关应当记入信用档案，向社会公布</p>	全国人大常委会， 2014-3-15	现行有效
《居民身份证法》（2011 年修订）	<p>第十九条 国家机关或者金融、电信、交通、教育、医疗等单位的工作人员泄露在履行职责或者提供服务过程中获得的居民身份证记载的公民个人信息，构成犯罪的，依法追究刑事责任；尚不构成犯罪的，由公安机关处十日以上十五日以下拘留，并处五千元罚款，有违法所得的，没收违法所得。单位有前款行为，构成犯罪的，依法追究刑事责任；尚不构成犯罪的，由公安机关对其直接负责的主管人员和其他直接责任人员，处十日以上十五日以下拘留，并处十万元以上五十万元以下罚款，有违法所得的，没收违法所得。</p> <p>有前两款行为，对他人造成损害的，依法承担民事责任。</p>	全国人大常委会， 2012-1-1	现行有效

续表

法律名称	具体规定	发布机构及生效时间	法律状态
《居民身份证法》(2011年修订)	第二十条 人民警察有下列行为之一的,根据情节轻重,依法给予行政处分;构成犯罪的,依法追究刑事责任:(一)利用制作、发放、查验居民身份证的便利,收受他人财物或者谋取其他利益的;(二)非法变更公民身份号码,或者在居民身份证上登载本法第三条第一款规定项目以外的信息或者故意登载虚假信息的;(三)无正当理由不在法定期限内发放居民身份证的;(四)违反规定查验、扣押居民身份证,侵害公民合法权益的;(五)泄露因制作、发放、查验、扣押居民身份证而知悉的公民个人信息,侵害公民合法权益的	全国人大常委会, 2012-1-1	现行有效
《电信和互联网用户个人信息保护规定》	全文规定	工业和信息化部, 2013-9-1	现行有效
《互联网用户账号名称管理规定》	第四条 互联网信息服务提供者应当落实安全管理责任,完善用户服务协议,明示互联网信息服务使用者在账号名称、头像和简介等注册信息中不得出现违法和不良信息,配备与服务规模相适应的专业人员,对互联网用户提交的账号名称、头像和简介等注册信息进行审核,对含有违法和不良信息的,不予注册;保护用户信息及公民个人隐私,自觉接受社会监督,及时处理公众举报的账号名称、头像和简介等注册信息中的违法和不良信息	中国互联网络信息中心, 2015-3-1	现行有效
《通信短信息服务管理规定》	第十四条 短信息服务提供者在业务活动中收集、使用用户个人信息,应当严格遵守有关法律法規的规定	工业和信息化部, 2015-6-30	现行有效
《寄送服务用户个人信息安全管理规范》	全文规定	国家邮政局, 2014- 3-26	现行有效
《测绘法》(2017年修订)	第四十七条 地理信息生产、保管、利用单位应当对属于国家秘密的地理信息的获取、持有、提供、利用情况进行登记并长期保存,实行可追溯管理;从事测绘活动涉及获取、持有、提供、利用属于国家秘密的地理信息,应当遵守保密法律、行政法规和国家有关规定;地理信息生产、利用单位和互联网地图服务提供者收集、使用用户个人信息的,应当遵守法律、行政法规关于个人信息保护的规定	全国人大常委会, 2017-7-1	现行有效



续表

法律名称	具体规定	发布机构及生效时间	法律状态
《中国人民银行关于银行金融机构做好个人金融信息保护工作的通知》	全文规定	中国人民银行， 2011-1-21	现行有效
《中国人民银行关于今日评机构进一步做好客户个人金融信息保护工作的通知》	全文规定	中国人民银行， 2012-3-27	现行有效
《征信业管理条例》	<p>第十三条 采集个人信息应当经信息主体本人同意，未经本人同意不得采集。但是，依照法律、行政法规规定公开的信息除外。企业的董事、监事、高级管理人员与其履行职务相关的信息，不作为个人信息。</p> <p>第十四条 禁止征信机构采集个人的宗教信仰、基因、指纹、血型、疾病和病史信息以及法律、行政法规规定禁止采集的其他个人信息。征信机构不得采集个人的收入、存款、有价证券、商业保险、不动产的信息和纳税数额信息。但是，征信机构明确告知信息主体提供该信息可能产生的不利后果，并取得其书面同意的除外。</p> <p>第十五条 信息提供者向征信机构提供个人不良信息，应当事先告知信息主体本人。但是，依照法律、行政法规规定公开的不良信息除外。</p> <p>第十六条 征信机构对个人不良信息的保存期限，自不良行为或者事件终止之日起为五年；超过五年的，应当予以删除。</p> <p>在不良信息保存期限内，信息主体可以对不良信息作出说明，征信机构应当予以记载。</p> <p>第十七条 信息主体可以向征信机构查询自身信息。个人信息主体有权每年两次免费获取本人的信用报告。</p> <p>第十八条 向征信机构查询个人信息的，应当取得信息主体本人的书面同意并约定用途。但是，法律规定可以不经同意查询的除外。</p> <p>征信机构不得违反前款规定提供个人信息。</p> <p>第十九条 征信机构或者信息提供者、信息使用者采用格式合同条款取得个人信息主体同意的，应当在合同中做出足以引起信息主体注意的提示，并按照信息主体的要求做出明确说明。</p>	国务院，2013-3-15	现行有效

续表

法律名称	具体规定	发布机构及生效时间	法律状态
《征信业管理条例》	第二十条 信息使用者应当按照与个人信息主体约定的用途使用个人信息，不得用作约定以外的用途，不得未经个人信息主体同意向第三方提供	国务院，2013-3-15	现行有效
《网络预约出租汽车经营服务管理暂行办法》	<p>第二十六条 网约车平台公司应当通过其服务平台以显著方式将驾驶员、约车人和乘客等个人信息的采集和使用的目的、方式和范围进行告知。未经信息主体明示同意，网约车平台公司不得使用前述个人信息用于开展其他业务。网约车平台公司采集驾驶员、约车人和乘客的个人信息，不得超越提供网约车业务所必需的范围。除配合国家机关依法行使监督检查权或者刑事侦查权外，网约车平台公司不得向任何第三方提供驾驶员、约车人和乘客的姓名、联系方式、家庭住址、银行账户或者支付账户、地理位置、出行线路等个人信息，不得泄露地理坐标、地理标志物等涉及国家安全的敏感信息。发生信息泄露后，网约车平台公司应当及时向相关主管部门报告，并采取及时有效的补救措施。</p> <p>第二十七条 网约车平台公司应当遵守国家网络和信息安全有关规定，所采集的个人信息和生成的业务数据，应当在中国内地存储和使用，保存期限不少于两年，除法律法规另有规定外，上述信息和数据不得外流</p>	交通部、工信部、公安部、商务部、工商总局、质检总局、国家网信办，2016-7-14	现行有效
《规范互联网信息服务市场秩序若干规定》	<p>第十一条 未经用户同意，互联网信息服务提供者不得收集与用户相关、能够单独或者与其他信息结合识别用户的信息（以下简称“用户个人信息”），不得将用户个人信息提供给他人，但是法律、行政法规另有规定的除外。互联网信息服务提供者经用户同意收集用户个人信息的，应当明确告知用户收集和处理用户个人信息的方式、内容和用途，不得收集其提供服务所必需以外的信息，不得将用户个人信息用于其提供服务之外的目的。</p> <p>第十二条 互联网信息服务提供者应当妥善保管用户个人信息；保管的用户个人信息泄露或者可能泄露时，应当立即采取补救措施；造成或者可能造成严重后果的，应当立即向准予其互联网信息服务许可或者备案的电信管理机构报告，并配合相关部门进行的调查处理</p>	工业和信息化部，2012-3-15	现行有效

续表

法律名称	具体规定	发布机构及生效时间	法律状态
《旅游法》（2016 年修订）	第五十二条 旅游经营者对其在经营活动中知悉的旅游者个人信息，应当予以保密	全国人大常委会， 2013-4-25	现行有效
《电子商务法（草案）》	<p>第四十五条 电子商务用户依法享有对其个人信息自主决定的权利。本法所称个人信息，是指电子商务经营主体在电子商务活动中收集的姓名、身份证件号码、住址、联系方式、位置信息、银行卡信息、交易记录、支付记录、快递物流记录等能够单独或者与其他信息结合识别特定用户的信息。</p> <p>第四十六条 电子商务经营主体收集用户个人信息，应当遵循合法、正当、必要原则，事先向用户明示信息收集、处理和利用的规则，并征得用户的同意。电子商务经营主体不得以拒绝为用户提供服务为由强迫用户同意其收集、处理、利用个人信息。禁止采用非法交易、非法入侵、欺诈、胁迫或者其他未经用户授权的手段收集个人信息。电子商务经营主体修改个人信息收集、处理、利用规则的，应当取得用户的同意。用户不同意的，电子商务经营主体应当提供相应的救济方法。</p> <p>第四十七条 用户有权查询与本人有关的个人信息。电子商务经营主体收到用户查询请求的，应当在核实身份后及时提供查询结果。用户对错误信息提出更正补充请求的，电子商务经营主体应当及时更正补充。</p> <p>第四十八条 电子商务经营主体对个人信息的处理和利用应当符合用户同意的处理利用规则。电子商务经营主体处理、利用个人信息的行为可能侵害用户合法权益的，用户有权请求电子商务经营主体中止相关行为。电子商务经营主体变更收集信息时约定的处理、利用的目的、方式和范围的，应当告知用户，并征得用户的明示同意。法定或者约定保存期限届满，电子商务经营主体应当主动或者按照用户的请求删除、停止处理和利用，或者销毁相关个人信息。</p> <p>第四十九条 电子商务经营主体应当建立健全内部控制制度和技术管理措施，防止信息泄露、丢失、毁损，确保电子商务数据信息安全。在发生或者可能发生用户个人信息泄露、丢失、毁损时，电子商务经营主体应当立即采取补救措施，及时告知用户，并向有关部门报告</p>	全国人大常委会， 2016-11-7	正式版本发布，未生效

## 二、个人信息保护的法规遵从建议

我国《网络安全法》已经颁布并实施，其中个人信息安全保护成为《网络安全法》的一大亮点，多项条款都从不同方面明确了对个人信息收集和保护的要求。第四十一条规定，网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。网络运营者不得收集与其提供的服务无关的个人信息，不得违反法律、行政法规的规定和双方的约定收集、使用个人信息，并应当依照法律、行政法规的规定和与用户的约定，处理其保存的个人信息。第四十二条规定：网络运营者不得泄露、篡改、毁损其收集的个人信息；未经被收集者同意，不得向他人提供个人信息。但是，经过处理无法识别特定个人且不能复原的除外。网络运营者应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失。在发生或者可能发生个人信息泄露、毁损、丢失的情况时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。第四十三条规定：个人发现网络运营者违反法律、行政法规的规定或者双方的约定收集、使用其个人信息的，有权要求网络运营者删除其个人信息；发现网络运营者收集、存储的其个人信息有错误的，有权要求网络运营者予以更正。网络运营者应当采取措施予以删除或者更正。第四十五条规定：依法负有网络安全监督管理职责的部门及其工作人员，必须对在履行职责中知悉的个人信息、隐私和商业秘密严格保密，不得泄露、出售或者非法向他人提供。可见，个人信息的收集、泄露、损坏、丢失个人信息的告知和报告制度、个人对其信息的删除权和更正权制度、网络安全监督管理机构及其工作人员对公民个人信息、隐私和商业秘密的保密制度成为个人信息保护的亮点性制度。个人信息保护《网络安全法》法规遵从具体框架如表 11-2 所示。

表 11-2 我国个人信息保护的法规遵从建议

控制项	个人信息保护的法规遵从建议	对应条款
1. 个人信息的收集		第四十一条 网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。
义务主体	<p>本条的义务主体为“网络运营者”，包括“网络的所有者、管理者和网络服务提供者”，其中网络服务提供者包括以下方面：</p> <ul style="list-style-type: none"><li>电信业务经营者，包括基础电信业务经营者、增值电信业务经营者和虚拟电信业务经营者。</li><li>互联网信息服务提供者。该类主体又分为两类，一类是经营性互联网信息服务，是指通过互联网向上网用户有偿提供信息或者网页制作等服务活动；另一类是非经营性互联网信息服务，是指通过互联网向上网用户无偿提供具有公开性、共享性信息的服务活动</li></ul>	<p>网络运营者不得收集与其提供的服务无关的个人信息，不得违反法律、行政法规的规定和双方的约定收集、使用个人信息，并应当依照法律、行政法规的规定和与用户的约定，处理其保存的个人信息。</p>
基本原则	<p>“合法、正当、必要的原则”包括以下方面：</p> <ul style="list-style-type: none"><li>合法性，即包括遵从法律和相关的行政法规，包括与个人信息保护相关的网络安全下位法。合法性原则要求个人信息相关行为应当符合现有法律法规要求，如经过权利人同意、履行法定义务，为提供服务而与第三方签订的协议，但该协议不得从事损害权利人的利益，且应严格遵循安全保障措施要求。</li><li>正当性，即即个人信息相关行为应当具备正当理由，如为服务之目的，履行职责之目的，为权利人之利益，为公共利益等，不应超出处理前所确定告知用户的目的。</li><li>必要性，即个人信息相关行为应以应确保为前述目的实现之必须。确保无过多处理，无不相关个人信息，不需要时及时删除等</li></ul>	<p>第四十二条 网络运营者不得泄露、篡改、毁损其收集的个人信息；未经被收集者同意，不得向他人提供个人信息。但是，经过处理无法识别特定个人且不能复原的除外。</p>
个人信息收集之“告知”	<p>收集前要采用个人信息主体易知悉的方式，向个人信息主体明确告知和警示如下事项：</p> <ul style="list-style-type: none"><li>处理个人信息的目的；</li><li>个人信息的收集方式和手段、收集的具体内容和留存时限；</li><li>个人信息的使用范围，包括披露或向其他组织和机构提供其个人信息的范围；</li><li>个人信息的保护措施；</li><li>个人信息管理者的名称、地址、联系方式等相关信息；</li><li>个人信息主体提供个人信息后可能存在的风险；</li><li>个人信息主体不提供个人信息可能出现的后果；</li><li>个人信息主体的投诉渠道；</li></ul>	<p>网络运营者应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失。在发生或者可能发生个人信息泄露、毁损、丢失的情况时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。</p>

续表

控制项	个人信息保护的法规遵从建议	对应条款
个人信息收集之“告知”	<ul style="list-style-type: none"> <li>如需将个人信息转移或委托于其他组织和机构,要向个人信息主体明确告知包括但不限于以下信息:转移或委托的目的、转移或委托个人信息的具体内容和使用范围、接受委托的个人信息获得者的名称、地址、联系方式等。</li> </ul> <p>遵从建议</p> <p>在实践中,企业均需要根据自身实际情况,在满足法律基本要求的前提下制定符合企业实际的隐私政策,避免盲目抄袭其他企业的规则,制定不切实际制定标准过高的隐私保护政策而引起违约或者行政处罚等法律风险</p>	<p>第四十三条 个人发现网络运营者违反法律、行政法规的规定或者双方的约定收集、使用其个人信息的,有权要求网络运营者删除其个人信息;发现网络运营者收集、存储的其个人信息有错误的,有权要求网络运营者予以更正。网络运营者应当采取措施予以删除或者更正。</p>
被收集者之“同意”	<p>处理个人信息前要征得个人信息主体的同意,包括默许同意或明示同意。</p> <ul style="list-style-type: none"> <li>默许同意。收集个人一般信息时,可认为个人信息主体默许同意,如果个人信息主体明确反对,要停止收集或删除个人信息。</li> <li>明示同意。收集个人敏感信息时,要得到个人信息主体的明示同意。</li> </ul> <p>网络经营者收集和使用用户的个人信息,应当以邀约和承诺的方式与个人订立合同,如果是网络运营商单方面发布的电子格式合同,合同的拟定者必须遵循公平原则,不得利用网络运营者的优势地位侵害公民个人的信息权利。</p>	<p>第四十五条 依法负有网络安全监督管理职责的部门及其工作人员,必须对在履行职责中知悉的个人信息、隐私和商业秘密严格保密,不得泄露、出售或者非法向他人提供</p>
2. 泄露、损坏、丢失个人信息的告知和报告制度		
不得泄露、篡改、毁损其收集的个人信息;未经被收集者同意,不得向他人提供个人信息	<p>电信业务经营者、互联网信息服务提供者应当采取以下安全保障措施防止用户个人信息泄露、毁损、篡改或者丢失:</p> <ul style="list-style-type: none"> <li>确定各部门、岗位和分支机构的用户个人信息安全管理责任;</li> <li>建立用户个人信息收集、使用及其相关活动的工作流程和安全管理;</li> <li>对工作人员及代理人实行权限管理,对批量导出、复制、销毁信息实行审查,并采取防泄密措施;</li> <li>妥善保管记录用户个人信息的纸介质、光介质、电磁介质等载体,并采取相应的安全储存措施;</li> <li>对储存用户个人信息的信息系统实行接入审查,并采取防入侵、防病毒等措施;</li> <li>记录对用户个人信息进行操作的人员、时间、地点、事项等信息;</li> <li>按照电信管理机构的规定开展通信网络安全防护工作;</li> <li>电信管理机构规定的其他必要措施。</li> </ul>	

续表

控制项	个人信息保护的法规遵从建议	对应条款
不得泄露、篡改、毁损其收集的个人信息；未经被收集者同意，不得向他人提供个人信息	<p>遵从建议</p> <ul style="list-style-type: none"><li>为确保合规，企业在实践中需要重点加强对手机号码、身份证号以及银行卡信息等敏感个人信息的保护，可采取的措施包括对工作人员实行权限管理，监督批量导出和复制行为。</li><li>在向第三方出售或者分享时，除非已获得用户的事先同意，这些企业需要对用户的个人信息提前进行匿名化处理，避免提供给第三方的信息可单独或者结合地识别用户身份信息，从而构成违法泄露个人信息。</li><li>此项禁止性规定对网络经营者而言会产生两项巨大的成本，一是声誉的损害，二是财务的损失。网络运营者必须采取“事先防范、事中控制和事后救济”三位一体的防护措施，关键是“事先防范”措施，确保不发生用户个人信息大面积泄露的</li></ul>	
发生或可能发生个人信息泄露、毁损、丢失的情况下应当采取的补救、告知和报告制度	<p>遵从建议</p> <p>考虑到通知用户可能对企业的商誉和业务造成致命影响，这一新规将促使企业更加重视数据安全保护</p>	
3. 个人对其信息的删除权和更正权制度		
删除请求权	<p>我国《网络安全法》规定的公民对其信息的删除权请求权主要有两种情形：</p> <ul style="list-style-type: none"><li>一是当事人发现网络运营商违反法律、行政法规或违反双方的约定收集和使用其信息；</li><li>二是网络运营商所收集的个人信息的目的已经消灭或双方约定的期限已经届满，在这两种情形下，当事人均有权要求网络运营商删除和停止使用其个人信息。</li></ul> <p>遵从建议</p> <ul style="list-style-type: none"><li>个人信息主体有正当理由要求删除其个人信息时，及时删除个人信息。删除个人信息可能影响执法机构调查取证时，采取适当的存储和屏蔽措施。</li><li>收集阶段告知的个人信息使用目的达到后，立即删除个人信息；如需继续处理，要消除其中能够识别具体个人的内容；如需继续处理个人敏感信息，要获得个人信息主体的明示同意。</li><li>超出收集阶段告知的个人信息留存期限，要立即删除相关信息；对留存期限有明确规定的，按相关规定执行。</li><li>个人信息管理者破产或解散时，若无法继续完成承诺的个人信息处理目的，要删除个人信息。删除个人信息可能影响执法机构调查取证时，采取适当的存储和屏蔽措施</li></ul>	

续表

控制项	个人信息保护的法规遵从建议	对应条款
更正权	公民对其错误信息的更正权，是指当事人发现网络运营商收集、存储的其个人信息有错误或者有缺失的，有权要求其补充或更正	
4. 网络安全监督管理机构及其工作人员对公民个人信息、隐私和商业秘密的保密制度		
个人信息的保密制度	<p>本条强调信息主体对于个人信息的保密权。信息保密权是个人信息自觉权的一种，是指本人得以请求信息处理主体保持信息隐秘性的权利。</p> <p>本条在于强调个人信息的保护主体除网络产品、服务的提供者，网络运营者外，依法负有网络安全监督管理职责的部门及其工作人员亦要严格保密其在履行职责过程中知悉的个人信息</p>	

第五节 监督管理与法律责任

我国《网络安全法》明确了个人信息保护的监督管理与相关法律责任。第八条规定：国家网信部门负责统筹协调网络安全工作和相关监督管理工作。国务院电信主管部门、公安部门和其他有关机关依照本法和有关法律、行政法规的规定，在各自职责范围内负责网络安全保护和监督管理工作。第六十四条规定：网络运营者、网络产品或者服务的提供者违反本法第二十二条第三款、第四十一条至第四十三条规定，侵害个人信息依法得到保护的权利的，由有关主管部门责令改正，可以根据情节单处或者并处警告、没收违法所得、处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款；情节严重的，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照。违反本法第四十四条规定，窃取或者以其他非法方式获取、非法出售或者非法向他人提供个人信息，尚不构成犯罪的，由公安机关没收违法所得，并处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款。

根据第八条，《网络安全法》规定了个人信息保护的监督管理制度，即“1+X”



模式：国家网信部门负责统筹协调网络安全工作，国务院电信主管部门、公安部门和其他有关机关依照本法和有关法律、行政法规的规定，在各自职责范围内负责网络安全保护和监督管理工作。同时，从规制行为来看，《网络安全法》第六十四条将以下两种行为入罪：一类是非法收集、使用个人信息行为；第二类是窃取或者以其他非法方式获取、非法出售或者非法向他人提供个人信息行为。从处罚责任来看，本条规定了网络运营者、网络产品和服务提供者违反本法关于个人信息保护的规定应该承担的法律后果，具体而言可从以下方面予以理解。

第一，由有关主管部门责令改正，同时可以根据情节单处或者并处警告、没收违法所得、处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。本条的处罚方式为警告、没收违法所得、罚款。罚款既包括对单位，也包括对直接责任人的罚款，数额从一万元到一百万元不等。《网络安全法》的亮点之一一是提升了对侵害个人信息违法行为的处罚力度。但由于我国《刑法》第二百五十三条也将“罚金”作为侵害个人信息犯罪的法定最低刑。根据 2000 年最高人民法院《关于适用财产刑若干问题的规定》，《刑法》没有明确规定罚金数额标准的，罚金的最低数额不能少于一千元，尽管法律对罚金刑的上限没有做限制性规定，但罚金最低数额与罚款最高数额的相差甚远，给司法适用制造了很大的困难，需要审慎执法。

第二，情节严重的，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照。所谓“情节严重”是指多次实施上述违法行为、违法收集、使用个人信息数量众多、经主管部门责令改正后拒绝予以改正等情形。

# 网络信息内容过滤

根据中国互联网违法和不良信息举报中心的统计，2017 年 4 月，在全国网络违法和不良信息举报中，淫秽色情类有害信息举报达 133.7 万件，占 45.9%；政治类有害信息举报占 30.8%；诈骗类有害信息举报占 4.0%；侵犯网民权益类有害信息举报占 7.4%；赌博类有害信息举报占 1.4%；暴恐类有害信息举报占 3.1%；网络敲诈和有偿删帖类有害信息举报占 0.3%；其他有害信息举报占 7.1%。腾讯、新浪、百度、阿里巴巴等主要商业网站受理违法和不良信息举报 202.4 万件，处置或向执法部门转交 202.4 万件。由此可以看出，对网络非法和有害信息的治理成为关乎整个网络安全和社会安全、甚至国家安全的重要任务。

从网络信息提供的整个流程来看，网络运营者网络信息流的重要控制者，是网络社会的重要环节，也是网络安全的“守门人”。因此，网络运营者对于网络安全具有天然的保护义务。由于网络具有公共产品的属性，它的非排他性决定了任何人都可以使用网络，这就造成网络中充斥着各种非法和有害信息。随着信息技术的发展，网络运营者对非法和有害信息治理的方式也在不断改进，因此，网络运营者应当承担与之能力相适应的内容治理义务。

网络运营者的治理义务的核心在于实现信息合法性、可用性、完整性和保密性等要求实施必要的安全保障及注意义务。依照网络运营者同用户之间的法律关系，注意义务可分为法定的注意义务与约定的注意义务，注意义务在“非法有

害信息”治理方面的具体内容则主要包含内容审查义务、配合政府部门执法义务、建立和完善投诉举报制度等。

## 第一节 《网络安全法》相关规定及释义

《网络安全法》第十二条对非法有害信息的范围进行了概括，第四十七、第四十八、第四十九、第五十条对非法有害信息的管理进行了规定，主要包括网络运营者对非法有害信息的治理责任、非法有害信息的举报制度以及监督管理等。对于来源于境外的非法有害信息的处理是《网络安全法》的创新性规定，为我国有效防范和处置来源于境外的非法有害信息提供了法律依据。

### 一、网络运营者的发现义务

《网络安全法》第四十七条和第四十八条对发现义务分别规定为“网络运营者应当加强对其用户发布的信息的管理，发现法律、行政法规禁止发布或者传输的信息的”，以及“电子信息发送服务提供者和应用软件下载服务提供者，应当履行安全管理义务，知道其用户有前款规定行为的，发现法律、行政法规禁止发布或者传输的信息的”。

从以上规定可以看出：第一，《网络安全法》对不同主题的发现义务进行了区分，即“电子信息发送服务提供者和应用软件下载服务提供者”与“网络运营商”的义务不同。因为网络运营商是针对公开发布的信息进行管理的，而电子信息发送服务提供者不能主动审查用户发送信息的内容，所以只能在因他人举报、主管机关告知或者其他情形下，知道用户发送的信息有违法内容时，才能采取相应的措施。第二，发现义务要求网络运营者发挥一种积极、主动的作用。通过对用户发布信息的监测、过滤、关键词识别等技术手段，对用户发布的信息附加合理的注意义务，防止违法或有害信息的扩散。第三，针对违法有

害信息的发现义务不同于一般侵权领域的义务。在一般侵权领域，网络服务提供者只需要负担“通知—删除”义务，即在被侵权人进行通知的情况下，采取删除、屏蔽、断开链接等必要措施，而对违法有害信息的“发现义务”更为严格。

## 二、非法有害信息治理的具有措施

### （一）及时发现与处置

网络运营者发现法律、行政法规禁止发布或者传输的信息的，应当立即停止传输该信息，采取消除等处置措施，防止信息扩散，保存有关记录，并向有关主管部门报告。这是对网络运营者在发现违法有害信息后的处理措施的规定。一方面要停止传输并消除该信息，另一方面还要积极预防有害信息的扩散。

关于“向有关主管部门报告”，根据《网络安全法》第八条的规定，国家网信部门负责统筹协调网络安全工作和相关监督管理工作。国务院电信主管部门、公安部门和其他有关机关依照本法和有关法律、行政法规的规定，在各自职责范围内负责网络安全保护和监督管理工作。县级以上地方人民政府有关部门的网络安全保护和监督管理职责，按照国家有关规定确定。《互联网信息服务管理办法》第十八条规定，国务院信息产业主管部门和省、自治区、直辖市电信管理机构，依法对互联网信息服务实施监督管理。新闻、出版、教育、卫生、药品监督管理、工商行政管理和公安、国家安全等有关主管部门，在各自职责范围内依法对互联网信息内容实施监督管理。

### （二）建立投诉与举报制度

举报是公众参与网络空间治理最直接、最便捷的重要途径。建立畅通、有效的举报渠道，有利于提高网民参与网络治理的积极性。《网络安全法》第十四条对向政府部门的举报进行了规定，任何个人和组织有权对危害网络安全的行为向网信、电信、公安等部门举报。收到举报的部门应当及时依法做出处理；不属于本部门职责的，应当及时移送有权处理的部门。《网络安全法》第四十九条在此基础

上,进一步要求网络运营者建立网络信息安全投诉、举报制度,公布投诉、举报方式等信息,及时受理并处理有关网络信息安全的投诉和举报。

从实践来看,2005 年国家设立中国互联网违法和不良信息举报中心,受理网民举报。目前全国 31 个省、自治区、直辖市网信办均已建立举报部门,监督、督促属地网站开展网络举报工作。

## 第二节 网络信息内容过滤制度概述

对网络信息内容进行管理是各国互联网管理的重要组成部分。而过滤是网络运营者最常采用的对违法有害信息内容进行识别的方式。各国根据历史文化传统、政治体制的不同,对有害信息会有不同的界定,范围和重点有所区别,但是一般来讲,违背公共道德,色情和暴力、危害国家安全,泄露国家秘密、网络犯罪等是各国监管的共同关注的对象。

### 一、非法有害信息的界定

在我国,“非法有害信息”的范围以“九不准”为基础,在不同的法律法规中有不同的表述。《网络安全法》第十二条从对“任何个人和组织”的义务的角度,对有害信息的范围进行了列举:“任何个人和组织使用网络应当遵守宪法法律,遵守公共秩序,尊重社会公德,不得危害网络安全,不得利用网络从事危害国家安全、荣誉和利益,煽动颠覆国家政权、推翻社会主义制度,煽动分裂国家、破坏国家统一,宣扬恐怖主义、极端主义,宣扬民族仇恨、民族歧视,传播暴力、淫秽色情信息,编造、传播虚假信息扰乱经济秩序和社会秩序,以及侵害他人名誉、隐私、知识产权和其他合法权益等活动。”

早在 2000 年全国人大常委会制定的《关于维护互联网安全的决定》中,从刑事责任的角度来对传播有害信息进行了规定:对有下列行为之一,构成犯罪的,

依照刑法有关规定追究刑事责任：①利用互联网造谣、诽谤或者发表、传播其他有害信息，煽动颠覆国家政权、推翻社会主义制度，或者煽动分裂国家、破坏国家统一；②通过互联网窃取、泄露国家秘密、情报或者军事秘密；③利用互联网煽动民族仇恨、民族歧视，破坏民族团结；④利用互联网组织邪教组织、联络邪教组织成员，破坏国家法律、行政法规实施。

《互联网信息服务管理办法》是互联网信息服务管理的核心法规，其中列举的“九不准”是网上“有害信息”治理最主要的规定。《互联网信息服务管理办法》第十五条规定，互联网信息服务提供者不得制作、复制、发布、传播含有下列内容的信息：①反对宪法所确定的基本原则的；②危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一的；③损害国家荣誉和利益的；④煽动民族仇恨、民族歧视，破坏民族团结的；⑤破坏国家宗教政策，宣扬邪教和封建迷信的；⑥散布谣言，扰乱社会秩序，破坏社会稳定的；⑦散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的；⑧侮辱或者诽谤他人，侵害他人合法权益的；⑨含有法律、行政法规禁止的其他内容的。

2000年与《互联网信息服务管理办法》同时出台的《电信条例》，也在第五章电信安全中的第五十六条规定：任何组织或者个人不得利用电信网络制作、复制、发布、传播“九不准”的信息，其内容与《互联网信息服务管理办法》相同。

其他一些行政法规基本都以“九不准”为基础进行了一些补充，例如，在《计算机信息网络国际联网安全保护管理办法》中增加了“损害国家机关信誉的”；《互联网上网服务营业场所管理条例》增加了“危害社会公德或者民族优秀传统文化的”等。互联网文化服务管理的相关规定中，对于服务提供者规定了“九不准”的要求，并且在“九不准”的基础上进行了补充。例如，《互联网文化管理暂行规定》规定互联网文化单位不得提供载有“有害信息内容”的文化产品，《互联网视听节目服务管理规定》视听节目不得含有的内容，在“九不准”的基础上都增加了“危害社会公德或者民族优秀传统文化的”规定。

总体来看，法律法规对于“非法有害信息”的界定分为三个层面：一是危害国家安全的消息，包括“煽动颠覆国家政权、推翻社会主义制度，煽动分裂国家、

破坏国家统一，宣扬恐怖主义、极端主义，宣扬民族仇恨、民族歧视”的信息等；二是危害社会稳定和秩序的信息，包括传播暴力、淫秽色情信息，编造、传播虚假信息扰乱经济秩序和社会秩序的信息等；三是对个人权利及其他私权利造成侵害的信息，包括侵害他人名誉、隐私、知识产权和其他合法权益的信息等。对于每类信息，法律没有规定明确的判断标准，需要网络运营者和监管机构在实践中形成合理的判断机制。

## 二、网络信息内容过滤

网络信息内容过滤，是指网络运营者发现违法有害信息的重要手段，而对有害信息进行封堵、过滤是各国通常都会采用的做法。例如，韩国对于国外的一些非法内容，特别是含有《国家安全法》（National Security Law）中规定的支持朝鲜的言论进行封堵。对于海外的、含有会给社会、文化和经济产生恶劣影响的非法信息（如色情、投机等）的网站，也会予以封堵。美国主要利用 IP 封堵等手段对不良内容进行过滤。政府对于不良网站的堵截方式通常是制定一个封堵用户登录的“互联网网址清单”，如果某网站被列入该清单，访问就会被自动禁止。美国 2000 年《未成年人互联网保护法》规定，中小学校、公共图书馆等必须在其网络服务程序的目录上提供过滤器，确保未成年人接触不到有色情内容的成人网站。政府建立了“E-Rate 计划”对学校、公共图书馆建立网络过滤技术系统提供资金支持，网络技术服务商在给学校和图书馆提供过滤技术服务时要给予优惠。日本内阁府于 2008 年颁布了《整顿青少年网络环境法》（全称为《为使青少年安全安心使用互联网，整顿网络环境法》，2008 年法律第 79 号）<sup>①</sup>。作为促进整顿青少年互联网使用环境的措施，日本内阁府、总务省、经济产业省联合开展了有害网站接入限制业务，即过滤业务。

网络运营者在网络过滤中发挥着重要作用。2017 年 5 月 3 日，Facebook 首席执行官马克·扎克伯格宣布，将在全球再雇 3 000 余人，这些新雇员将和现有的 4 500 人组成网站社区运营团队，在世界范围内监控每周所有用户上传的数以

<sup>①</sup> 参考日本内阁府网站 <http://www.cao.go.jp/>。

百万条的内容，更快地发现并处理那些包含仇恨犯罪和伤害儿童内容的视频和帖子。欧洲大规模的 ISP 审查首先在英国展开，英国电信监管机构 Ofcom 报告称：英国所有主要网络运营商目前均提供网络层面的过滤，帮助父母保护孩子免受有害网络信息。2017 年 7 月，德国要求社交媒体必须在 24 小时内找到明显包含非法仇恨言论的帖子并予以删除，否则将被处以重罚。对于在澳大利亚境外的内容，澳大利亚通信与媒体管理局（Australian Communications and Media Authority, ACMA）有权对在澳大利亚境内托管的互联网内容进行限制，并制定海外网站的“黑名单”提供给过滤软件。

事实上，有害信息很难全部消除。首先，信息数量呈指数级增长是长期存在的趋势，网络运营者面临的是海量的审查；其次，违法有害信息的存在形式多种多样，或者在不同的情境之下有不同的含义，机器过滤无法完全识别，最终还是有赖于人工去实际甄别，而人工审核也不可避免存在局限性，难以穷尽；最后，海量的审核以及对网络运营者违法有害信息“发现”义务的增加，有可能加重对个人信息权利侵害的风险。

目前常用的过滤手段分为两类，一类为基于网络爬虫或搜索引擎的主动监测系统，另一类是基于关键词过滤的被动防御技术。随着技术的发展，关键词过滤已经不仅针对文本，还可以针对图像、声音、视频，甚至出现了智能过滤技术。2017 年，Google 宣布将使用更多的机器学习和人工智能技术甄别极端视频，并提供数据表明，AI 在 75% 的情况下，都能比人类先甄别极端视频。调查人员表明，AI 能够处理的视频数量是人类的两倍，而且这个差距随着系统升级会越来越大。Google 的人工智能将被用来判断被举报的视频，例如仇恨言论、攻击性和暴力视频。

### 第三节 网络信息内容过滤法规遵从框架及建议

根据《网络安全法》的要求，对于违法有害信息的处理，网络运营者在具体的业务运营中可以遵从表 12-1 的建议。



表 12-1 网络信息内容过滤的法规遵从建议

控制项	网络信息内容过滤的遵从要求	对应条款
履行发现义务	<p>形成有害信息的判别标准：建立并动态更新修改关键词库，根据非法有害信息的特点进行分类，将不同分类置于不同场景之中，注明危险等级，建立对应的发现处置机制。</p> <p>提升有害信息发现的技术水平，从关键词过滤、黑白名单以及过滤器等针对文字的识别方式逐步向特征识别、基于大数据的人工智能识别演进发展。</p> <p>建立人工审核团队：在技术过滤存在疑问时，转至人工审核团队；加强人员培训，提升有害信息的识别能力。</p> <p>建立有害信息审核规则：形成及时发现和处置的机制和流程，技术审核后无法识别或有较大嫌疑的转给人工审核团队，由人工审核团队进行进一步审核，以发现、甄别和处理。</p> <p>完善网络安全技术措施：采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施</p>	<p>第四十七条 网络运营者应当加强对其用户发布的信息的管理，发现法律、行政法规禁止发布或者传输的信息的，应当立即停止传输该信息，采取消除等处置措施，防止信息扩散，保存有关记录，并向有关主管部门报告</p>
开展有害信息处置	<p>形成完善的有害信息处置流程：根据前端有害信息识别的内容，删除有害信息，并对有害信息的来源进行追查，采取相应的防范措施。</p> <p>建立严格的内控流程，保护用户信息，防止数据泄露；加强内部监督管理，防止内部人员利用删帖权限非法牟利。</p> <p>对来自境外的有害信息进行处置：对于企业来讲，发现来源于境外的非法有害信息，应当通知有关机构</p>	<p>第四十八条 任何个人和组织发送的电子信息、提供的应用软件，不得设置恶意程序，不得含有法律、行政法规禁止发布或者传输的信息。</p> <p>电子信息发送服务提供者和应用软件下载服务提供者，应当履行安全管理义务，知道其用户有前款规定行为的，应当停止提供服务，采取消除等处置措施，保存有关记录，并向有关主管部门报告。</p> <p>第五十条 国家网信部门和有关部门依法履行网络信息安全监督管理职责，发现法律、行政法规禁止发布或者传输的信息的，应当要求网络运营者停止传输，采取消除等处置措施，保存有关记录；对来源于中华人民共和国境外的上述信息，应当通知有关机构采取技术措施和其他必要措施阻断传播</p>

续表

控制项	网络信息内容过滤的遵从要求	对应条款
积极配合执法	建立举报、投诉中心，开通举报、投诉渠道，公开电话、邮箱等信息，并对接到的举报、投诉内容进行受理和处理。  对于已经被相关主管部门立案调查的情况下：开展自查自纠。网络运营者应积极开展自查自纠，排查企业在有害信息处理规则、技术手段、人工审核等各方面可能存在的问题和漏洞；配合执法调查。配合相关主管部门，有违法有害信息立即采取停止传输、消除等处置措施	第四十九条 网络运营者应当建立网络信息安全投诉、举报制度，公布投诉、举报方式等信息，及时受理并处理有关网络信息安全的投诉和举报。  网络运营者对网信部门和有关部门依法实施的监督检查，应当予以配合

第四节 监督管理与法律责任

一、监督管理

（一）监督管理的主体

《网络安全法》第五十条规定：国家网信部门和有关部门依法履行网络信息安全监督管理职责，发现法律、行政法规禁止发布或者传输的信息的，应当要求网络运营者停止传输，采取消除等处置措施，保存有关记录。国家网信部门是互联网内容的主管部门，具体对于互联网内容的监管是在中央网络安全和信息化领导小组的统筹下，由国家互联网信息办公室协调工业和信息化部、公安部、文化部、国家新闻出版广电总局等相关部门在各自职责范围内开展对互联网违法有害信息的监督管理。

国家互联网信息办公室成立于 2011 年，其主要职责包括落实互联网信息传播方针政策和推动互联网信息传播法制建设，指导、协调、督促有关部门加强互联网信息内容管理，负责网络新闻业务及其他相关业务的审批和日常监管，指导有关部门做好网络游戏、网络视听、网络出版等网络文化领域业务布局规划，协调有关部门做好网络文化阵地建设的规划和实施工作，负责重点新闻网站的规划建

设,组织、协调网上宣传工作,依法查处违法违规网站,指导有关部门督促电信运营企业、接入服务企业、域名注册管理和服务机构等做好域名注册、互联网地址(IP地址)分配、网站登记备案、接入等互联网基础管理工作,在职责范围内指导各地互联网有关部门开展工作。

《网络安全法》对网络运营者对监管部门的配合义务做了原则规定:“网络运营者对网信部门和有关部门依法实施的监督检查,应当予以配合。”《反恐怖主义法》第十六条也规定了有关单位协助的义务,第十九条第二款规定,网信、电信、公安、国家安全等主管部门对含有恐怖主义、极端主义内容的信息,应当按照职责分工,及时责令有关单位停止传输、删除相关信息,或者关闭相关网站、关停相关服务。有关单位应当立即执行,并保存相关记录,协助进行调查。

在国外对网络信息内容的监督管理大体也呈现多主体的格局,所不同的是有些国家管理部门相对分散,有些则较为集中。例如美国采取了较为分散的模式,联邦通信委员会负责对网上色情淫秽信息内容分类分级的管理机构,商务部国家电信和信息管理局是学校、图书馆互联网有害信息内容限制接入技术措施的政策评估机关,联邦调查局、联邦移民和海关局、美国邮政检查局、司法部儿童虐待和色情工作组等都是儿童色情犯罪活动的刑事执法机关。澳大利亚则是较为集中模式的代表,其政府分级委员会负责对内容进行分级,通信与媒体管理局是互联网内容审查的主要管理部门。

## (二) 对来源于境外有害信息的处理

对来源于境外的有害信息,《网络安全法》和《反恐怖主义法》都做了相应规定:对来源于中华人民共和国境外的上述信息,应当通知有关机构采取技术措施和其他必要措施阻断传播。对互联网上跨境传输的含有恐怖主义、极端主义内容的信息,电信主管部门应当采取技术措施,阻断传播。

从防止境外有害信息流入境内的渠道上来看,阻止境外有害信息通过互联网向境内传播是控制境内有害信息流通的重要手段。这两条规定对我国处理来源于境外的有害信息所采取的必要技术措施提供了重要的法律依据。

## 二、法律责任

在行政执法实践中已有网络运营者因未及时履行发现义务受到相应处罚。2017年8月初，东北大学毕业生李某在BOSS直聘遭遇招聘诈骗、深陷传销组织致死事件引发社会广泛关注，经北京市网信办、天津市网信办的调查，BOSS直聘在为用户提供信息发布服务过程中，违规为未提供真实身份信息的用户提供了信息发布服务；未采取有效措施对用户发布传输的信息进行严格管理，导致违法违规信息扩散。网信办认定BOSS直聘的上述行为已违反《网络安全法》第二十四条、第四十八条规定，并依据第六十一条、第六十八条规定，下达了行政执法检查记录，责令网站立即开展自查整改，完善内容审核管理机制，严格加强对各类招聘信息发布主体及发布信息真实性的审核管理，全面清理各类违法违规信息。此案是网信办依据《网络安全法》处罚网络运营者不履行治理义务的第一案。由此可以看出，网络运营者履行网络信息内容治理义务的重要性。

2017年8月11日，国家网信办指导北京市、广东省网信办分别对腾讯微信、新浪微博、百度贴吧立案，并依法展开调查。经北京市、广东省网信办初查，3家网站的微信、微博、贴吧平台分别存在有用户传播暴力恐怖、虚假谣言、淫秽色情等危害国家安全、公共安全、社会秩序的信息。3家网站平台涉嫌违反《网络安全法》等法律法规，对其平台用户发布的法律法规禁止发布的信息未尽到管理义务。

从具体的法律规定来看，网络运营者在内容管理方面的行政责任主要由《网络安全法》第六十八条、六十九条规定构成。《网络安全法》第六十八条规定，网络运营者违反本法第四十七条规定，对法律、行政法规禁止发布或者传输的信息未停止传输、采取消除等处置措施、保存有关记录的，由有关主管部门责令改正，给予警告，没收违法所得；拒不改正或者情节严重的，处十万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。电子信息发送服务提供者、应用软件下载服务提供者，不履行本法第四十八条第二款规定的安全管理义务的，依照前款规定处罚。第六十九条规

定，网络运营者违反本法规定，有下列行为之一的，由有关主管部门责令改正；拒不改正或者情节严重的，处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员，处一万元以上十万元以下罚款：①不按照有关部门的要求对法律、行政法规禁止发布或者传输的信息，采取停止传输、消除等处置措施的；②拒绝、阻碍有关部门依法实施的监督检查的；③拒不向公安机关、国家安全机关提供技术支持和协助的。

对于其他任何组织或个人，第七十条规定，发布或者传输本法第十二条第二款和其他法律、行政法规禁止发布或者传输的信息的，依照有关法律、行政法规的规定处罚。

除此之外，在2002年发布的《互联网信息服务管理办法》中也对制作、复制、发布、传播有害信息以及互联网信息服务提供者分别规定了行政责任，其中第二十条规定，制作、复制、发布、传播本办法第十五条所列内容之一的信息，构成犯罪的，依法追究刑事责任；尚不构成犯罪的，由公安机关、国家安全机关依照《中华人民共和国治安管理处罚条例》（以下简称《治安管理处罚条例》）、《计算机信息网络国际联网安全保护管理办法》等有关法律、行政法规的规定予以处罚；对经营性互联网信息服务提供者，并由发证机关责令停业整顿直至吊销经营许可证，通知企业登记机关；对非经营性互联网信息服务提供者，并由备案机关责令暂时关闭网站直至关闭网站。



# Part 3

## 第三部分

### 关键信息基础设施运营者 的网络安全法律遵从

第 13 章 关键信息基础设施的界定及其范围

第 14 章 安全保护义务

第 15 章 网络安全审查

第 16 章 数据本地化与跨境传输

第 17 章 网络安全信息共享





# 关键信息基础设施的 界定及其范围

## 第一节 国外关键信息基础设施概念的界定及其范围

### 一、美国

美国对关键基础设施的概念一直沿用的是 2001 年《爱国者法案》第 1016 节的规定：所谓“关键基础设施”是指对美国重要的物理或虚拟的系统和资产，此类系统和资产的功能丧失或被破坏将对国家安全、国家经济安全、国家公众健康与安全或上述事项的任何组合产生削弱影响。2013 年《改善关键基础设施的网络安全行政令》指出：“关键基础设施”是指对美国非常重要的物理或虚拟的系统和资产。如果这类系统或资产被破坏或丧失工作能力，将对美国的安全，国家经济安全，国家公众健康或公共安全，或者任何这些事项的集合产生削弱影响，其重申了 2001 年《爱国者法案》中对关键基础设施概念的界定。2009 年《国家基础设施保护计划》（2009 NIPP）中对于国家关键信息基础设施进行了规定：电子的信息和通信系统以及这些系统中的信息，其中信息和通信系统由对各类型数据进行处理、储存和通信的软硬件所组成，包括计算机信息系统、控制系统和网络。

“9·11”事件的冲击，使得美国高度重视关键基础设施的保护，加之其关键基础设施信息化程度较高，因此，历年来针对网络安全问题出台的一系列立法、战略和行政令都紧紧围绕着关键基础设施的保护。关键基础设施所依赖的信息和通信系统以及其整体已经涵盖了关键信息基础设施的范围，因而在美国，通常更多地用关键基础设施保护问题指代关键信息基础设施保护问题。

克林顿政府于1996年发布的第13010号行政令中规定，关键基础设施部门主要包括电信、电力系统、天然气及石油的存储和运输、银行和金融、交通运输、供水系统、紧急服务（包括医疗、警察、消防、救援）、政府连续性8类。布什政府于2003年发布的《关键基础设施和重要资产物理保护国家战略》中，将美国关键基础设施部门划分为11类：农业与食品、水、公共卫生、应急服务、国防工业基地、通信、能源、交通运输、金融、化学工业与有害物质、邮政与货运。2003年第7号总统令《关键基础设施标识、优先级和保护》中，确认了17类国家重要基础设施和关键资源，主要包括：信息技术，电信，化学品，商业设施，大坝，商用核反应堆、原料和废料，政府设施，交通系统（包括公共交通、航空、海运、陆路/内河航运、铁路和管道系统），应急服务，邮政和货运服务，农业和食品，饮用水和废水处理系统，公共健康和医疗，能源[包括石油和天然气的生产、提炼、储存和输送及电力（商用核电设施除外）]，银行和金融，国家纪念碑和象征性标志，国防工业基地。2006年发布的《国家基础设施保护计划》和2007年发布的《国土安全战略》均对前述17类关键基础设施进行确认。2008年，国土安全部宣布增加“关键制造业”作为第18类需要保护的国家关键基础设施。2013年2月，奥巴马政府发布的第21号总统令《提高关键基础设施的安全性和恢复力》重新确定了16类关键基础设施部门，包括：化学，商业设施，通信，关键制造，水利，国防工业基地，应急服务，能源，金融服务，食品和农业，政府设施，医疗保健和公共卫生，信息技术，核反应堆、材料和废弃物，运输系统，水及污水处理系统。

从美国发布的国家战略和法律法规可以看出，美国对关键基础设施和重要资源部门的分类正趋向稳定，其根据对国家关键基础设施和重要资源的重要性评估不断更新与调整其确定的部门种类，以满足国家安全保障的实际需要。总体而言，美国认为关键基础设施包括物理和虚拟的资产与系统，并且指出关键基础设施对于国家安全、经济安全、公众健康或公共安全具有重要性和不可替代性，并将此

作为确定关键基础设施和重要资源清单，以及国家基础设施是否具备“关键性”的认定标准。同时，国土安全部将采用统一的标准来确定对关键基础设施的定级，并将定级结果与特定领域机构协商后，秘密告知所有者或运营者，并且负责对关键基础设施进行年度审核检查，将报告报送总统。

## 二、欧盟

2005 年的《保护关键基础设施的欧洲计划》将关键信息基础设施定义为关键基础设施本身或关键基础设施运营必不可少的 ICT（Information and Communication Technology）系统（电信、计算机/软件、互联网、卫星等）。由此可以看出，关键信息基础设施是关键基础设施的组成部分，一旦确定了关键基础设施的范围，即确定了关键信息基础设施的范围。而欧盟针对关键基础设施的概念界定则主要根据 2004 年 10 月 20 日发布的《打击恐怖主义活动，加强关键基础设施保护的通信》中的规定：关键基础设施是指如果被破坏或摧毁，会对公民的健康、安全、稳定或经济福祉或成员政府的有效运转造成严重影响的物理和信息技术设施、网络、服务和资产。关键基础设施横跨经济的诸多部门和重要政府服务。之后，2006 年的《关于欧盟理事会制定识别、指定欧洲关键基础设施，并评估提高保护的必要性指令的建议》指出，“关键基础设施”是指那些为维护包括供应链、健康、平安、安全、经济或人民社会福祉在内的关键社会职能必不可少的资产或其中一部分。2007 年的《关于建立作为安全和自由防卫总战略中 2007—2013 “对恐怖主义和相关安全风险的预防，准备和结果控制” 的具体战略的第 2007/124/EC 号决定》进一步指出，“关键基础设施”包括那些物质资源、服务、信息技术设施、网络和基础设施资产，如果其被破坏或毁灭，将对关键社会功能（包括供应链、健康、保险、安全、人民经济或社会的安宁，或者共同体或成员的机能）产生严重的冲击。

2013 年，欧洲委员会发布的《关于对关键信息基础设施攻击的网络犯罪公约委员会第六号指引》中，再一次将关键基础设施定义为对国家至关重要的物理或虚拟的系统及资产，其不能有效运转、丧失功能或者受到损毁会对国家安全和防御、经济安全、公共健康及安全，以及其他这些问题的多个方面造成削弱影响。该指引指出，关键基础设施包括能源、食品、水利、资源、交通、财

政、工业、国防以及政府或公共服务部门，在这一概念的基础上将运行关键基础设施的计算机系统，包括诸如工业控制系统和监控与数据采集系统等在内的系统等归为关键信息基础设施。由此可见，关键信息基础设施的概念在原来的基础上得到了进一步的拓展，但关键信息基础设施范围的界定依然在关键基础设施的范围之内。

2016年7月6日，欧盟通过了《关于欧盟共同的高水平网络与信息系统安全措施的指令》（简称NIS指令），于2016年8月8日正式生效，欧盟各成员要在2018年5月9日之前将其转化为国内法。指令并没有采用“关键基础设施”的概念，而是使用了“基本服务运营者”的表述。所谓“基本服务运营者”，是指“提供继续关键社会活动及/或经济活动基本服务的主体，该服务的提供依赖于网络和信息系统，网络安全事件会对该服务的提供造成重大的破坏性影响”，涉及能源（电力、石油及天然气），运输（航空、铁路、水运及陆运），银行，金融市场基础设施，医疗卫生，饮用水供应和分配，以及数字基础设施（互联网交换点、域名系统服务提供者及顶级域名注册）领域。

欧盟委员会在《欧洲关键基础设施保护计划绿皮书》中将关键基础设施部门确定为以下11类，包括：①能源（石油和天然气生产、提炼、处理和储藏，其中包括输送管道，发电，输电，供电，天然气和石油）；②信息和通信技术（信息系统和网络保护、设备自动化和控制系统，互联网，固定电信服务，移动电信服务，无线电通信和导航，卫星通信，广播）；③水（饮用水供应，控制水质，控制水量）；④食品（食品供应和食品安全保护）；⑤健康（医疗和医院护理，药品、血清、疫苗和药物，生物实验室和生物制剂）；⑥金融系统〔支付服务/支付体系（私有），政府财政调配〕；⑦公共和法律秩序与安全（维持公共和法律秩序、安全和稳定，司法和拘留管理）；⑧民事管理（政府职能、武装部队、民事管理服务，应急服务，邮政和快递服务）；⑨交通（公路交通，铁路交通，航空运输，内河航运，远洋和近海航运）；⑩化学和核工业〔化学和核材料的生产、储存/加工，危险物品（化学材料）的输送管道〕；⑪太空和研究。由此可见，欧盟委员会确立了十一大类关键基础设施部门，并且分别列明了各关键基础设施部门的子部门及其中涉及的产品和服务。相较美国确定的关键基础设施部门而言，欧盟的关键基础设施部门清单更加具体和详细，这一细化对欧盟各个成员据此确定其本国的关键基础

设施部门来说具有很强的指导性和可操作性。

### 三、英国

英国将国家关键基础设施称为关键国家基础设施（Critical National Infrastructure, CNI），并将其界定为由不间断向国家提供基本服务而言不可或缺的关键元素组成的国家基础设施。没有这些元素，就不能提供基本服务，英国将遭到严重的经济损失、巨大的社会破坏乃至严重的生命威胁。同时，英国政府始终致力于保护关键国家基础设施免受两种威胁：针对物理设施的物理攻击和针对计算机或通信系统的电子攻击。由此可见，与美国类似，英国的关键国家基础设施既包括物理层面也包括虚拟层面的基础设施。

英国确定了 10 类关键基础设施部门，参照欧盟委员会确定的关键基础设施部门清单，英国确定了其本国的关键基础设施部门及其子部门，包括：通信（数字通信、固定语音通信、邮递、政府信息、无线通信），应急服务（救护、消防和营救、海上急救、警察），能源（电力、天然气、石油），金融（资产管理、金融设施、投资银行、市场、小额银行），食品（生产、进口、加工、配送、零售），政府和公共服务（中央政府、地区政府、地方政府、议会和立法机关、司法、国家安全），公共安全（化学、生物、辐射和核恐怖袭击、危及公民生活的事件），健康（医疗保健、公共卫生），交通（航空、海运、铁路、公路），水（饮用水、污水）。

### 四、法国

在法国，对于维持社会和经济运行至关重要的所有基础设施都被视为关键基础设施。由此可见，法国的关键基础设施保护范围十分广泛，只要是对社会和经济运行至关重要的基础设施都被视为关键基础设施，但是并未明确“至关重要”的认定标准或方法。

法国确定了 12 类关键基础设施部门，参照欧盟委员会确定的关键基础设施部门清单，法国确定了其本国的关键基础设施部门，包括金融，工业，能源，司法，医疗保健，国家政府机构，电子通信、影声媒介和信息技术，交通系统，

供水，食品，空间和研究，武装部队，但是并未具体细化上述关键基础设施部门的子部门。

## 五、德国

德国对关键信息基础设施的主要界定则因考虑政府和社会在总体上严重依赖基础设施的安全运转，从而提出了关键基础设施的关键性考虑要素，即凡是其故障会导致供应短缺或给大部分人口造成灾难性后果的元素都被定义为关键的。在此基础上，德国进一步明确指出，关键基础设施是指对社会具有重大意义，其故障或损坏会导致持续的供给短缺，导致公共秩序的重大中断或造成其他严重后果的基础设施。针对信息基础设施，2005 年的《信息基础设施保护国家计划》对其定义为给定基础设施中 IT 部分的总和。2015 年的《德国网络安全法》吸收了德国 2011 年的《网络安全国家战略》中关于“关键信息基础设施”的定义，指出关键信息基础设施是指对公共生活安全具有重大影响的设施或机构，这些设施或机构一旦被损害或破坏，将对整个社会的公共秩序产生难以估计的影响。

德国的关键基础设施部门清单不断调整，德国最初参照欧盟委员会确定的关键基础设施部门清单，确定了其本国的关键基础设施部门，包括：交通运输，能源，危险材料，电信和信息技术，金融、货币和保险系统，供应（包括供水、食品供应、医疗保健、应急和营救服务），政府机构、公共管理和司法系统，新闻媒体、研究机构和文化资产共八大类。随后，德国根据现实需要，对已经确定的关键基础设施部门进行定期评估，调整其范围，目前被确定为关键基础设施的部门包括：能源、信息技术和通信、运输、卫生、水利、食品、金融和保险部门、政府和行政机构、媒体和文化。2015 年的《德国网络安全法》明确：凡是涉及水资源、能源、通信、医疗、交通、金融、保险等与德国民众日常生活紧密相关的行业或企业均属于关键基础设施的保护范围。

## 六、日本

2005 年的《关键基础设施信息安全措施行动计划》规定，关键基础设施是指由提供高度不可代替且对人民生活和社会经济活动不可获取的服务的商业实体组

成。如果基础设施的功能被暂停、削弱或根本无法运行，人们的社会生活和经济活动会遭到重大破坏。在此基础上，日本明确指出，组成关键基础设施重要部分的基本信息系统统称为“关键信息系统”，若其遭到破坏，将对公民社会生活和经济活动造成不可估量的损失。

日本政府认为，电信、金融、民航、铁路、电力、燃气、政务、医疗、水利和物流这 10 个关键领域从事着不可替代的服务，若其信息系统遭到破坏，会对公民社会生活和经济活动造成不可估量的损失。因此，日本政府将这些领域认定为关键基础设施部门，在其国家战略来推行中，详细区分这些领域中的哪些系统属于重点保护对象，并制定了一系列战略来保障这些关键基础设施部门的信息安全。目前，在日本新近颁布的《网络安全战略》中，关于受保护的关键信息基础设施的范围已有所扩大，其借鉴美国的关键基础设施保护类型，将智慧城市、交通控制系统、其他网络类型的系统、国防工业、能源相关产业的信息系统也看作关键基础设施对待。2015 年的《关键信息基础设施保护基本政策》中确定关键信息基础设施包括：信息和通信服务、金融服务、航空服务、铁路服务、电力供应服务、供气服务、政府和行政服务、医疗服务、供水服务、物流服务、化学工业、信用卡服务、石油工业共 13 个领域。

## 七、新加坡

最初确立的关键基础设施部门包括 6 类，即银行和金融、信息和电信、能源、水、交通、医疗保健。2002 年后，经过相应的审查和评估，为了满足反恐的需求，在上述 6 类关键基础设施部门的基础上，新加坡政府又增加了食品供应、航空安全和海运安全 3 类关键基础设施部门。由此可见，新加坡关键基础设施部门的确定同样不是最终的和不变的，那些被列为清单的关键基础部门将不断经过政府相关部门的审查和评估，根据维护国家安全的现实需求进行相应的调整和更新。

在确定关键基础设施部门的过程中，上述很多国家都以首次在官方文件中按照具体商业或工业部门确定关键基础设施的美国总统关键基础设施保护委员会为模板，将“部门”作为分析单位，基本遵循了现有商业/工业部门的界定，并反映

了大多数基础设施都由私有参与者拥有和经营的事实。因此，在决定哪些关键基础设施部门应被纳入关键基础设施保护清单时，不仅需要各级政府专家和官员的意见，还需要征求私有部门专家的意见。纵观国外关键信息基础设施保护立法，欧盟非常精确地确定了关键基础设施部门、子部门，以及由这些部门提供的产品和服务，其他国家如美国、英国、德国、法国、日本、新加坡都基本确定了关键基础设施部门的范围，其中美国确定的关键基础设施部门的范围最为广泛，并且包括关键基础设施和重要资源两部分。然而，各国关键基础设施部门范围的差异不仅产生于其对关键概念认定的差异，而且还产生于具体国家的特性和传统的差异。社会政治因素，以及地理和历史前提都决定了某个部门是否应被视为关键。上述各国最多提到的关键基础设施部门大多是现代化社会的核心部门，同时也是大规模破坏将造成极大灾难的部门，主要包括：银行和金融、中央政府/政府服务、（电信）通信/信息和通信技术、应急/营救服务、能源/电力、医疗保健服务、交通/供应/配送、水（供应）。

同时，基于对各国不同时期确定的关键基础设施部门可以分析得出，关键基础设施部门的“关键性”概念本身在不断变化，确定有资格成为关键对象的基础设施部门的准则也随着时间的推移在不断扩展。例如，美国确定的关键基础设施部门从最初的8类发展成为目前的16类，部门类别基本增加了一倍，其中，一些基础设施部门被新认定为关键基础设施部门，一些关键基础设施部门经过调整成为其他关键基础设施部门的子部门，还有一些关键基础设施部门经过合并共同形成新的关键基础设施部门。由此可见，各国在不同时期内对关键基础设施部门的认定都处于不断进行调整和更新的动态过程中，以满足维护国家安全、反恐、执法或促进经济发展的实际需要。

## 第二节 我国关键信息基础设施概念的提出及范围界定

近年来，面对严峻的网络安全形势，我国高度重视关键基础设施保护。2015



年 7 月 1 日颁布实施的《国家安全法》在第二十五条<sup>①</sup>部署了有关关键基础设施和重要领域信息系统及数据安全可控的战略举措。

2016 年 11 月，全国人大常委会发布了《网络安全法》，其中在“网络运行安全”一般规定的基础上设专节对关键信息基础设施的运行安全做出了具体规定，并实行重点保护。这是在我国立法中首次明确规定了关键信息基础设施的定义和具体保护措施。

我国在 2015 年 7 月公布的《网络安全法（草案）》中，将关键信息基础设施定义为：提供公共通信、广播电视传输等服务的基础信息网络，能源、交通、水利、金融等重要行业和供电、供水、供气、医疗卫生、社会保障等公共服务领域的重要信息系统，军事网络，设区的市级以上国家机关等政务网络，用户数量众多的网络服务提供者所有或管理的网络和系统。保护的范围包括基础信息网络、重要行业和领域的重要信息系统、军事网络、重要政务网络、用户数量众多的商业网络等。

而在 2016 年颁布的《网络安全法》中，第三十一条采用了“列举+概括”的形式，将关键信息基础设施界定为：公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护，并规定其具体范围和安全保护办法由国务院制定。

此外，《网络安全法》进一步提出了关键信息基础设施保护的三同步原则，明确了关键信息基础设施保护主管部门的职责和运营者的安全保护义务，建立了关键信息基础设施运营者采购网络产品、服务的安全审查制度，并要求建立关键信息基础设施保护相关部门之间的协作机制等。

需要指出的是，《网络安全法》采用了“关键信息基础设施”的表述，容易让人误解我国只保护电信业和信息技术业的关键基础设施，但其实与我国保护能源、

<sup>①</sup> 第二十五条 国家建设网络与信息安全保障体系，提升网络与信息安全保护能力，加强网络和信息技术的创新研究和开发应用，实现网络和信息核心技术、关键基础设施和重要领域信息系统及数据的安全可控；加强网络管理，防范、制止和依法惩治网络攻击、网络入侵、网络窃密、散布违法有害信息等网络违法犯罪行为，维护国家网络空间主权、安全和发展利益。

交通、水利、金融等所有领域关键基础设施重要信息系统的立法目的不符。既然我国立法已经采用这一表述，应该将“关键信息基础设施”解释为：既包括电信业和信息技术业的关键基础设施，也包括其他行业关键基础设施的信息系统。对于关键信息基础设施具体范围的划定，因“国家安全”存在较大的解释空间，可能出现宽泛界定和狭义界定两种情形。

2016年12月27日，经中央网络安全和信息化领导小组批准，国家互联网信息办公室发布《国家网络空间安全战略》。《国家网络空间安全战略》指出，“国家关键信息基础设施是指关系国家安全、国计民生，一旦数据泄露、遭到破坏或者丧失功能可能严重危害国家安全、公共利益的信息设施，包括但不限于提供公共通信、广播电视传输等服务的基础信息网络，能源、金融、交通、教育、科研、水利、工业制造、医疗卫生、社会保障、公用事业等领域和国家机关的重要信息系统，重要互联网应用系统等。”

2017年7月11日，《关键信息基础设施安全保护条例》（征求意见稿）第十八条沿用了《网络安全法》第三十一条的规定，通过“非穷尽列举行业和领域+危害后果”的方式，给出了关键信息基础设施的范围：“下列单位运行、管理的网络设施和信息系统，一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的，应当纳入关键信息基础设施保护范围：①政府机关和能源、金融、交通、水利、卫生医疗、教育、社保、环境保护、公用事业等行业领域的单位；②电信网、广播电视网、互联网等信息网络，以及提供云计算、大数据和其他大型公共信息网络服务的单位；③国防科工、大型装备、化工、食品药品等行业领域科研生产单位；④广播电台、电视台、通讯社等新闻单位；其他重点单位。”

在判定流程上，中央网络安全和信息化领导小组办公室于2016年6月编制的《国家网络安全检查操作指南》具有较强的参考意义，即关键信息基础设施判定的三步法：一是确定关键业务，二是确定支撑关键业务的信息系统或工业控制系统，三是根据关键业务对信息系统或工业控制系统的依赖程度，以及信息系统发生网络安全事件后可能造成的损失认定关键信息基础设施。

此外，主要行业关键业务的确定如表 13-1 所示。

表 13-1 主要行业关键业务的确定

行业		关键业务
能源	电力	电力生产（含火电、水电、核电等） 电力传输 电力配送
	石油石化	油气开采 炼化加工 油气输送 油气储存
	煤炭	煤炭开采 煤化工
金融		银行运营 证券期货交易 清算支付 保险运营
交通	铁路	客运服务 货运服务 运输生产 车站运行
	民航	空运交通管控 机场运行 订票、离港及飞行调度检查安排 航空公司运营
	公路	公路交通管控 智能交通系统[一卡通、电子不停车收费系统（Electronic Toll Collection, ETC）收费等]
	水运	水运公司运营（含客运、货运） 港口管理运营 航运交通管控
水利		水利枢纽运行及管控 长距离输水管控 城市水源地管控
医疗卫生		医院等卫生机构运行 疾病控制 急救中心运行
环境保护		环境监测及预警（水、空气、土壤、核辐射等）
工业制造 （原材料、装备、消费品、电子制造）		企业运营管理 智能制造系统（工业互联网、物联网、智能装备等） 危化品生产加工和存储管控（化学、核等） 高风险工业设施运行管控

续表

行业	关键业务
市政	水、暖、气供应管理 城市轨道交通 污水处理 智慧城市运行及管控
电信与互联网	语音、数据、互联网基础网络及枢纽 域名解析服务和国家顶级域注册管理 数据中心/云服务
广播电视	电视播出管控 广播播出管控
政府部门	信息公开 面向公众服务 办公业务系统

### 第三节 我国关键信息基础设施的界定主体

《网络安全法》第三十二条规定了关键信息基础设施分行业、分领域主管部门负责制，明确规定：负责关键信息基础设施安全保护工作的部门，要按照国务院规定的职责分工，分别编制并组织实施本行业、本领域的关键信息基础设施安全规划，指导和监督关键信息基础设施运行安全保护工作。

2017 年的《关键信息基础设施安全保护条例（征求意见稿）》确立了各部门统筹协调、分工负责的监管机制，所涉及的监管部门包括国家网信部门、国家行业主管或监管部门、国务院公安、国家安全、国家保密行政管理、国家密码管理部门以及县级以上地方人民政府有关部门等。其中，国家网信部门负责统筹协调关键信息基础设施的安全保护工作和相关监督管理工作，为关键信息基础设施保护实施的核心部门。国家行业主管或监管部门按照国务院规定的职责分工，负责指导和监督本行业、本领域关键信息基础设施安全保护工作。国务院公安、国家安全、国家保密行政管理、国家密码管理等部门以及各级人民政府依照各自职责或者国家有关规定负责或者开展关键信息基础设施安全保护。此外，《关键信息基础设施安全保护条例（征求意见稿）》第十九条第三款还强调了专家在认定关键信息基础设施过程中的作用，以提高关键信息基础设施认定的准确性、合理性和科学性。

## 第 14 章

# 安全保护义务

在信息化社会，关键信息基础设施安全已经成为网络空间安全的命脉所在，深刻影响国家安全、社会正常运转乃至公民的生存权和发展权。然而，在全球范围内，针对关键信息基础设施的网络攻击及破坏性网络安全事件却在不断上演<sup>①</sup>。2016 年 4 月 19 日，习近平总书记在网络安全和信息化工作座谈会上的讲话指出，我国的关键信息基础设施面临着来自不同层面上的安全威胁：首先，由于网络空间的开放性和互联互通，既有少数国家层面的有组织、有计划的入侵攻击和窃密，也有黑客个人的网络攻击，还有犯罪团伙、商业间谍、邪教组织、恐怖分子等有组织行为，给我国的关键信息基础设施带来巨大的风险；其次，由于我国许多基础信息网络和重要信息系统的核心设备、技术和高端服务主要依赖国外进口，因此关键信息基础设施安全防护能力较弱，一些“命门”受制于人，应对网络威胁的能力整体不足，无法抵御大规模、有组织的网络攻击。关键信息基础设施运营者是国家网络安全及个人信息安全的守门人，其提供的服务与产品具有公共产品

<sup>①</sup> 2007 年，爱沙尼亚国会、政府部门及银行遭到网络攻击，技术专家们发现攻击来源于一个庞大的“僵尸网络”，涉及位于 178 个国家和地区的大约 8.5 万台计算机，其中绝大多数计算机是在被黑客入侵和操纵的情况下，无辜和毫不知情地卷入了有关攻击；2010 年伊朗政府遭到“震网”病毒的攻击及 2014 年乌克兰政府遭到的网络攻击等极大地危害了国家的安全；2014 年 4 月 9 日爆发的 OpenSSL 心脏出血（Heart bleed）漏洞，以及 2014 年 8 月 31 日匿名黑客利用苹果 iCloud 上的云服务漏洞发动网络攻击，导致用户个人信息的泄露；2016 年 3 月，全球有 2/3 的网站服务器用的开源加密工具 OpenSSL 爆出安全漏洞——“水牢漏洞”，这一漏洞允许“黑客”攻击网站，并读取密码、信用卡账号、商业机密和金融数据等加密信息，对全球网站产生巨大的安全考验，我国有 10 万余家网站受到影响；2016 年 7 月 15 日，安全研究人员发现一个名为 cuteRansomware 的新恶意勒索软件，该恶意软件代码的注释及勒索内容全部使用的中文，这意味着该勒索软件只将中国用户作为攻击目标。

属性。在此背景之下，确立与完善关键信息基础设施运营者的安全保护义务应为网络安全法律制度体系建设的中中之重。

## 第一节 《网络安全法》相关规定及释义

我国《网络安全法》对于关键信息基础设施运营者的安全保护义务做出了明确的规定，主要从两个层面予以规定。

首先，第二十一条明确规定：国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：①制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；②采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施；③采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；④采取数据分类、重要数据备份和加密等措施。本条主要规定了等级保护制度对于关键信息基础设施运营者安全保护义务的“基线”安全义务要求。本条是关于关键信息基础设施运营者应该履行的最基础的安全保护义务，即网络安全等级保护制度的相关要求。第一，制定内部安全管理制度及内部操作规程，指定网络安全负责人，落实网络安全保护责任。网络安全运营者应该根据法律、行政法规及网络安全等级保护制度的规定，制定企业内部的安全管理规章，落实义务性规定，明确相关机构和人员的职责。第二，采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施。该技术措施应该具有有效性，例如安装毒防病毒软件、网络身份认证系统、网络入侵检测系统、网络风险审计系统等，防范网络入侵与攻击事件的发生。第三，采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月。网络日志留存对于检测计算机运行状态，调查网络犯罪具有重要的作用。网络日志的种类众多，留存期限应该根据具体实际确定，但是本法规定应不少于六个月。第四，采取数据分类、重要数据备份和加密等措施。数据分类就是

把具有某种共同属性或特征的数据归并在一起，通过其类别的属性或特征来对数据进行区别。重要数据备份是容灾的基础，是指为防止系统出现操作失误或系统故障导致数据丢失，而将全部或部分数据集合从应用主机的硬盘或阵列复制到其他的存储介质中的过程。数据加密是指通过加密算法和加密密钥将明文转变为密文，以实现数据的保密性。

此外，《网络安全法》第三十四条规定：除本法第二十一条的规定外，关键信息基础设施的运营者还应当履行下列安全保护义务：①设置专门安全管理机构和安全管理负责人，并对该负责人和关键岗位的人员进行安全背景审查；②定期对从业人员进行网络安全教育、技术培训和技能考核；③对重要系统和数据库进行容灾备份；④制定网络安全事件应急预案，并定期进行演练；⑤法律、行政法规规定的其他义务。本条针对关键信息基础设施的运行安全明确规定了关键信息基础设施运营者更高层面的安全保护义务，包括“人”的安全保护义务和对“系统”的安全保护义务。对人的安全包括完善网络安全管理体系和对从业人员的教育、培训和考核。对“系统”的安全保护义务包括对重要数据和数据库的容灾备份，以保障关键信息基础设施在遇到突发事件时能够稳定运行，保证业务的连续性，确保数据安全。同时，应制定应急预案并进行演练，以提升应急机制的有效性。

## 第二节 关键信息基础设施运营者 安全保护义务制度概述

### 一、关键信息基础设施运营者的概念及识别

网络运营者是一个内涵和外延都相当广泛的概念，既包括一般性的网络运营者，又包括关键信息基础设施运营者。2017年6月1日起正式施行的《网络安全法》首次正式提出了“网络运营者”的概念<sup>①</sup>。《网络安全法》第七十六条规定：

<sup>①</sup> 在已经失效的《电信服务标准（试行）》中出现过“网络运营者”，但主要指提供通道、电路段的网络服务提供商，与《网络安全法》中的网络运营者并非同一概念。

网络运营者，是指网络的所有者、管理者和网络服务提供者。从法条表述可以看出，网络运营者这一概念的内涵确定，而外延相对开放。《网络安全法》条文中“网络运营者”这一术语出现了 31 次，“网络运营者”的安全保护义务有 14 个条文予以规定，“网络运营者”的法律责任有 5 个条文予以规定。

关键信息基础设施运营者是一般性网络运营者中的特殊和重要类别，也是立法规制的重点。我国《网络安全法》在第三章第二节中用了相当的篇幅规范了关键信息基础设施的安全与保护法律制度，涵盖了公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域。《网络安全法》第三十一条规定：国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护，关键信息基础设施的具体范围和安全保护办法由国务院制定。这是我国首次在法律层面提出关键信息基础设施的概念和重点保护范围。随后，《关键信息基础设施保护条例（草案）》出台，企业界、学界的呼声呼吁关键信息基础设施运营者的识别步骤应尽快确立，例如先识别一定的行业，然后识别一些重点的服务领域及业务，再识别这些领域中系统和信息系统一类设施的部分。

## 二、关键信息基础设施运营者网络安全保护义务的特殊性分析

鉴于关键信息基础设施国家网络安全守门人的特殊地位，其既有责任也有能力向所有的网络用户提供安全保护。这是一种最低限度的法律义务。关键信息基础设施运营者的安全保护义务具有如下特点。

第一，从法律义务的分类来看，该项义务是具有法律强制力保障实施的作为性、复合性义务。关键信息基础设施安全涉及业务连续性、自主可控与数据安全三个宏观层面的问题。《网络安全法》对于以上问题予以足够的关注。首先，《网络安全法》充分认识到了业务连续能力对于关键信息基础设施的重要性，规定了关键信息基础设施运营者日常的安全维护义务，其既要遵循安全等级保护制度对



一般信息系统的安全要求，也要履行更加严格的安全维护义务，包对“人”的安全义务和对“系统”的安全义务两个方面；其次，在自主可控与数据安全层面，《网络安全法》对于关键信息基础设施供应链安全及数据存留方面做出了特殊的规定，要求关键信息基础设施的运营者采购网络产品和服务，可能影响国家安全的这些网络产品和服务应当通过国家安全审查。采购这些网络产品和服务时，关键信息基础设施运营者应当按照规定与提供者签订安全保密协议，明确安全和保密义务与责任。

第二，从法律义务的主体来看，该义务属于具有复合主体的义务规范。根据《网络安全法》第七十六条规定，网络运营者是指网络的所有者、管理者和网络服务提供者。关键信息基础设施运营者可理解为关键信息基础设施的所有者、管理者和服务的提供者，其义务主体具有复合性特征。《网络安全法》对于关键信息基础设施管理者和服务提供者的责任和义务的规定比较明确和全面，对国家（所有者）在关键信息基础设施安全保护中的责任规定较为单一。

第三，从法律义务的生成来看，该项义务内生于关键信息基础设施成立之时，贯穿于其为网络用户提供网络服务的全部过程，即使在其退出网络服务领域之时，也需为该义务的履行做出最为妥善的安排。关键信息基础设施运营者在经营过程中，如果要停止某项技术服务，对于使用该技术的所有用户应当提前发出通知，及时提醒其继续使用将带来的风险，以及告知其避免这些风险需要采用的措施，给用户足够的时间进行技术更换工作<sup>①</sup>。网络服务提供者之所以在其技术服务结束时仍需向用户承担信息安全保障义务，源于长久以来两者之间的一种相互生存依赖，在当下的互联网行业，某类网络服务提供者在某些技术方面长期处于垄断地位，导致其地位已具有不可替代性，因而在退出时理应采取一些安全措施，保护所有使用其技术服务用户的安全，避免因其退出技术服务而给用户带来人身及财产损失。

第四，该义务应具有一定“合理限度”。尽管我国还未明确关键信息基础设施的识别程序与标准，但不可否认，关键信息基础设施运营者并非公益机构，必将

<sup>①</sup> 例如，微软中国宣布于 2014 年 4 月 8 日停止对 Windows XP 的支持，但考虑到该操作系统在我国通信等重要行业仍占据较高比例，若立即停止将给基础通信网络带来直接风险，威胁基础通信网络的整体安全，故其决定与包括腾讯在内的国内领先的互联网安全及防病毒厂商密切合作，为中国全部使用 Windows XP 的用户，在用户选择升级到新一代操作系统之前，继续提供独有的安全保护，帮助用户安全度过系统过渡期。

承载着“安全”与“发展”这一看似矛盾的价值诉求，需要在网络安全保护义务的内容设定及其合理限度中需求平衡，在实践中应与其技术能力与业务范围相适应与匹配。

### 三、美国关键信息基础设施运营者安全保护义务的法律规制“特色”分析

美国是网络大国与强国，美国的关键信息基础设施保护立法一直成为世界各国的标杆，对我国关键信息基础设施运营者，甚至是一般企业，在网络安全保护义务履行中具有借鉴意义。在美国，一般性企业和关键信息基础设施运营者都负有履行网络安全保护义务的职责，但鉴于立法在技术发展中的滞后性及监管者与企业信息获取上的不对称性等原因，美国没有单一立法明确规定企业应该采取什么样的安全措施以确保企业得到足够的安全保障，但在不同层面立法中明确企业的安全保护义务<sup>①</sup>已成为趋势。具体而言，企业层面的安全保护义务具有如下显著的特点。

#### （一）立法渊源广泛，历时久远

美国企业的安全保护义务的立法渊源广泛，主要包括联邦、州层面的法律法规、普通法及侵权法、合同承诺、商业标准及政府规章、国际法律法规及执法行动等。联邦及州层面的成文法律法规在赋予企业一般性网络安全义务方面的立法和法规数量众多。在联邦立法层面，相关立法主要包括以下内容。美国1999年的《统一电子交易法案》（Uniform Electronic Transactions Act, UETA）规定了网络服务商在信息传播中的安全程序步骤，以及在电子记录传播过程中由于未能采取适当的安全措施预防或阻止错误的产生时应承担的责任，即规定了采取适当安全措施预防或阻止错误的产生是网络服务商的法定义务。2001年的Gramm-Leach-Bliley安全规则法案中开始对金融业强加一种执行安全措施的综合性义务，该法案要求

---

① 美国的法律和法规中可使用“安全”、“保障”等措辞，例如欧盟数据保护指令与HIPAA；在另一种情况下，也可使用与“安全”相关的一些词语，如“认证”、“完整性”、“机密性”及“数据可用性”等措辞，例如E-SIGN, UETA, UN Electronic Communications Convention。

金融机构执行一个综合性的书面信息安全计划，包括：①确保信息安全和消费者信息的保密性；②保护信息不被盗用、破坏以及信息的可靠性；③保护信息不被非法地访问和使用。2002 年 9 月 18 日，布什政府发布的国家网络空间安全战略提出了布什政府保障美国公共部门和私人企业信息系统安全不受故意、恶意破坏的计划，并且加强了国家对信息安全的重视和关注。战略规定：企业有义务采取适当安全措施以保障第三方的信息系统、网络和数据安全，如果第三方遭到损害是因为企业怠于履行该种信息安全义务所导致的，那么企业应当承担对第三方损害进行赔偿的法律责任。此外，提出了企业应当对内部信息安全的安全职责和安全义务进行评估，如保障网络空间安全的义务应当成为企业董事会与 CEO 层面重视和关注的问题。2003 年，美国网络空间安全国家战略提出确保网络空间安全是一项难度很大的战略挑战，要求整个社会（联邦、州和地方政府、私有部门和美国人民）共同关注和合作。由于网络技术的互联互通性，保障网络信息安全需要全社会的共同努力。此后的国家安全战略也多次提到过应通过政府、企业、个人的合作共同应对信息安全难题。

## （二）网络安全保护义务的主体为“所有企业”，“所有企业”应该负有“恰当”、“合理”的安全保护义务

鉴于立法在技术发展中的滞后性及监管者与企业与信息获取上的不对称性等原因，美国没有单一立法明确规定企业应该采取什么的安全措施以确保企业得到足够的安全保障，而是在现有立法中规定一般性网络安全保护义务的主体为“所有企业”，保护客体涵盖“所有的公司数据”，所有企业应该负有“恰当”、“合理”的安全保护义务。究其原因：首先，网络信息技术的快速发展导致了立法的滞后性问题；其次，存在政府和监管部门与网络运营者信息的不对称性问题。被监管对象掌握对自身所处环境所面临的风险，以及运营各环节等方面的一手信息和知识，监管者如果强行施加统一的、具体的、措施性的安全义务，很可能造成事倍功半甚至力道用错了地方的局面。

此外，所有的企业所履行的安全义务标准应该是在实践中可发展的，应重视“程序性”。所谓法律标准性实际就是指法律的“程序性”，包括：识别被保护的资产；进行风险控制：识别与评估资产威胁、脆弱性与损失，考虑可获得的选择；

发展与实施已确定的安全计划，如风险评估与安全控制；持续性监控、再评估与调试，以确保有效性及解决新的威胁、脆弱性及选择等。

### （三）在网络安全保护义务设定中，明确了利益相关者的责任机制

所有企业网络安全义务的责任机制主要包括董事会及高级管理人员的安全治理责任、公司对于安全漏洞的披露责任、怠于履行义务应承担的法律责任等。以董事会及高级管理人员的安全治理责任为例，2003 年 12 月，美国国土安全部在加利福尼亚州圣克拉拉市联合主办了一次“国家网络安全峰会”，会议的直接成果在于创建了 5 个由私有部门组成的特别工作组，其中包括法人治理工作组。在其报告中，该工作组号召所有的组织、机构应将法人信息安全治理作为公司在董事会层面优先考虑的事项。承担董事会及高级管理人员的安全治理责任的企业董事会和 CEO 应负有以下责任：①审议并通过安全计划；②监督信息安全计划的发展、执行和维持；③要求提供有关安全计划执行的整体情况、公司对相关法规的执行情况和有关安全计划事务的定期报告（至少每年一次），以及公开风险评估报告、风险管理和控制决定、测试结果、破坏或妨害安全的表现和处理对策，以及对信息安全计划中新变化的介绍。

## 第三节 关键信息基础设施运营者安全保护义务 法规遵从框架及建议

### 一、关键信息基础设施运营者安全保护义务法规遵从框架

关键信息基础设施运营者安全保护义务来源于法律和法规的强制性规定。我国关键信息基础设施安全保护义务的相关法律法规主要包括综合及重要领域类规定两大部分，数量众多。为保障上述制度的有效实施，一方面，以国家互联网信息办公室（以下简称“网信办”）为主的监管部门制定了配套法规；另一方面，全国信息安全标准化技术委员会（以下简称“信安标委”）同时制定并公开了一系列

以信息安全技术为主的重要标准的征求意见稿，为网络运营者提供了非常具有操作性的合规指引。

关键信息基础设施运营者的“基线”安全保护义务首先来源于等级保护制度的基本要求。信安标委在原有的信息系统安全等级保护制度的基础之上，发布了包括《网络安全等级保护实施指南》、《网络安全等级保护基本要求》等在内的多项标准文件的征求意见稿。考虑到现行的《信息安全等级保护管理办法》已不适用《网络安全法》的要求，新的《网络安全等级保护管理办法》也正在制定中。

同时，随着《关键信息基础设施安全保护条例》、《信息安全技术关键信息基础设施安全检查评估指南》等征求意见稿的公布，关键信息基础设施运营者的安全保护义务得以进一步明确。总体来说，我国关键信息基础设施安全保护义务的主要法规遵从框架如表 14-1 所示。

表 14-1 关键信息基础设施运营者安全保护义务法规遵从框架

法律名称	法律规定	发布机构及发布时间	法律状态
《网络安全法》	<p>第二十一条 国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：</p> <p>（一）制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；（二）采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施；（三）采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；（四）采取数据分类、重要数据备份和加密等措施；</p> <p>第三十四条 除本法第二十一条的规定外，关键信息基础设施的运营者还应当履行下列安全保护义务：</p> <p>（一）设置专门安全管理机构和安全管理负责人，并对该负责人和关键岗位的人员进行安全背景审查；（二）定期对从业人员进行网络安全教育、技术培训和技能考核；（三）对重要系统和数据库进行容灾备份；（四）制定网络安全事件应急预案，并定期进行演练；（五）法律、行政法规规定的其他义务</p>	全国人大常委会 2016 年 11 月 7 日	现行有效

续表

法律名称	法律规定	发布机构及发布时间	法律状态
《关键信息基础设施安全保护条例（征求意见稿）》	<p>第二十一条 建设关键信息基础设施应当确保其具有支持业务稳定、持续运行的性能，并保证安全技术措施同步规划、同步建设、同步使用。</p> <p>第二十二条 运营者主要负责人是本单位关键信息基础设施安全保护工作第一责任人，负责建立健全网络安全责任制并组织落实，对本单位关键信息基础设施安全保护工作全面负责。</p> <p>第二十三条 运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障关键信息基础设施免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：（一）制定内部安全管理制度和操作规程，严格身份认证和权限管理；（二）采取技术措施，防范计算机病毒和网络攻击、网络侵入等危害网络安全行为；（三）采取技术措施，监测、记录网络运行状态、网络安全事件，并按照规定留存相关的网络日志不少于六个月；（四）采取数据分类、重要数据备份和加密认证等措施。</p> <p>第二十四条 除本条例第二十三条外，运营者还应当按照国家法律法规的规定和相关国家标准的强制性要求，履行下列安全保护义务：（一）设置专门网络安全管理机构和网络安全管理负责人，并对该负责人和关键岗位人员进行安全背景审查；（二）定期对从业人员进行网络安全教育、技术培训和技能考核；（三）对重要系统和数据库进行容灾备份，及时对系统漏洞等安全风险采取补救措施；（四）制定网络安全事件应急预案并定期进行演练；（五）法律、行政法规规定的其他义务。</p> <p>第二十五条 运营者网络安全管理负责人履行下列职责：（一）组织制定网络安全规章制度、操作规程并监督执行；（二）组织对关键岗位人员的技能考核；（三）组织制定并实施本单位网络安全教育和培训计划；（四）组织开展网络安全检查和应急演练，应对处置网络安全事件；（五）按规定向国家有关部门报告网络安全重要事项、事件。</p> <p>第二十六条 运营者网络安全关键岗位专业技术人员实行执证上岗制度。执证上岗具体规定由国务院人力资源社会保障部门会同国家网信部门等部门制定。</p> <p>第二十七条 运营者应当组织从业人员网络安全教育培训，每人每年教育培训时长不得少于1个工作日，关键岗位专业技术人员每人每年教育培训时长不得少于3个工作日</p>	国家互联网办公室	正式版未发布，未生效

续表			
法律名称	法律规定	发布机构及发布时间	法律状态
《网络安全法》	<p>第二十八条 运营者应当建立健全关键信息基础设施安全检测评估制度，关键信息基础设施上线运行前或者发生重大变化时应当进行安全检测评估。</p> <p>运营者应当自行或委托网络安全服务机构对关键信息基础设施的安全性和可能存在的风险隐患每年至少进行一次检测评估，对发现的问题及时整改，并将有关情况报国家行业主管或监管部门。</p> <p>第二十九条 运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照个人信息和重要数据出境安全评估办法进行评估；法律、行政法规另有规定的，依照其规定</p>	全国人大常委 2016 年 11 月 7 日	现行有效

关键信息基础设施运营者除遵从以上安全保护义务之外，同时还应关注信安标委颁布的诸多标准，如《信息安全技术关键信息基础设施安全检查评估指南（征求意见稿）》、《关键信息基础设施识别指南》、《信息安全技术关键信息基础实施网络安全保护要求》、《信息安全技术网络安全等级保护实施指南（征求意见稿）》等。

## 二、关键信息基础设施运营者安全保护义务法规遵从建议

我国《网络安全法》第三十一条和第三十四条明确规定了关键信息基础设施安全保护义务的基本内容要求。第二十一条是“等级保护”制度的相关规定。

本条根据网络安全等级保护制度，对网络运营者的安全保护义务做了基本的规定，主要包括：制定内部安全管理制度和操作流程、采取防范网络安全行为的技术措施、配备相应的硬件和软件检测、采取数据分类、重要备份和数据加密。第三十四条规定了关键信息基础设施运营者应该履行的安全保护义务，主要内容包括：完善网络安全管理体系；采取多种方式、定期对从业人员进行网络安全教育、技术培训和技能考核，提高从业人员的网络安全意识和网络安全技术能力；对重要系统和数据库进行容灾备份；制定网络安全应急预案，并定期进行演练，以提高应急工作人员的能力及工作的有效性。具体法规遵从建议如表 14-2 所示。

表 14-2 关键信息基础设施运营者安全保护义务法规遵从建议

控制项	关键信息基础设施运营者安全保护义务法规遵从建议	对应条款
1. 完善内部网络安全管理体系		第二十一条 国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：
设置专门安全管理机构和安全管理负责人	<p>设置专门安全管理机构，具体承担网络安全管理工作，负责组织落实网络安全管理制度和网络安全技术防护措施，建立健全岗位网络安全责任制度，明确岗位及人员的网络安全责任。具体而言建议如下：</p> <ul style="list-style-type: none"> <li>● 设立或强化专门的网安技术部门与政策/法规部门，或放入现有的合规、内控、法务、支持部门，并在组织架构（图）中体现。</li> <li>● 顶层设计一般应不低于副总级别，或专职首席信息官（Chief Information Officer, CIO）/首席战略官（Chief Strategy Officer, CSO）/首席信息安全官（Chief Information Security Officer, CISO）等。应明确无论如何设定组织架构，管理层应对网络安全承担最终责任。</li> <li>● 应在制度、（劳动、聘用）合同和岗位职责描述中写明（和区分人员的）职责义务、绩效考核和违反后果、责任追究等</li> </ul>	<p>（一）制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；（二）采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施；（三）采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；（四）采取数据分类、重要数据备份和加密等措施；（五）法律、行政法规规定的其他义务。</p>
对该负责人和关键岗位的人员进行安全背景审查	<p>对安全管理机构负责人和关键岗位人员的身份、背景和专业资格等进行审查。具体建议如下：</p> <ul style="list-style-type: none"> <li>● 应至少有一份标准的背景调查清单，并对实际填写予以保存。清单填写事项应经外部验证，并可重复验证（体现持续和更新）</li> </ul>	第三十四条 除本法第二十一条的规定外，关键信息基础设施的运营者还应当履行下列安全保护义务：
2. 从业人员的网络安全教育、技术培训和技能考核		（一）设置专门安全管理机构和安全管理负责人，并对该负责人和关键岗位的人员进行安全背景审查；
从业人员网络安全教育、技术培训和技能考核	<p>遵从具体建议如下：</p> <ul style="list-style-type: none"> <li>● 应至少有一份培训、考核的年度计划与题目内容，并记录实施和验证培训、考核的效果；</li> <li>● 外包或通过网络的，应有合同或可在线印证</li> </ul>	（二）定期对从业人员进行网络安全教育、技术培训和技能考核；（三）对重要系统和数据库进行容灾备份；（四）制定网络安全事件应急预案，并定期进行演练；（五）法律、行政法规规定的其他义务。
3. 对重要系统和数据库的容灾备份		第三十九条 国家网信部门应当统筹协调有关部门对关键信息基础设施的安全保护采取下列措施：
对重要系统和数据库的容灾备份	<p>具体的遵从建议如下：</p> <ul style="list-style-type: none"> <li>● 对重要系统和数据库的容灾备份应监测、记录网络运行状态、网络安全事件，网络日志留存六个月以上。</li> <li>● 根据数据的重要性及其对系统运行的影响，制定数据的备份策略和恢复策略，明确应备份信息的备份方式、备份频度、存储介质、保存期等。</li> <li>● 应有日志服务器和区分职责的专人管理，实现自动化与人工结合的事件甄别和处理痕迹验证。</li> </ul>	<p>（一）对关键信息基础设施的安全风险进行抽查检测，提出改进措施，必要时可以委托网络安全服务机构对网络存在的安全风险进行检测评估；（二）定期组织关键信息基础设施的运营者进行网络安全应急演练，提高应对网络安全事件的水平和协同配</p>



续表

控制项	关键信息基础设施运营者安全保护义务法规遵从建议	对应条款
4. 制定应急预案与演练		合能力；（三）促进有关部门、关键信息基础设施的运营者以及有关研究机构、网络安全服务机构等之间的网络安全信息共享；（四）对网络安全事件的应急处置与网络功能的恢复等，提供技术支持和协助
制定应急预案与演练	发生网络安全事件，立即启动应急预案。具体建议如下： <ul style="list-style-type: none"><li>按照要求采取技术措施和其他必要措施，消除安全隐患，防止危害扩大，并向有关主管部门报告。</li><li>应有对启动和实施应急预案的培训、演练、整改记录。</li></ul>	

第四节 监督管理与法律责任

《网络安全法》对于关键信息基础设施运营者违反或怠于履行安全保护义务的监督管理与法律责任做出了明确的规定。《网络安全法》第八条规定，国家网信部门负责统筹协调网络安全工作和相关监督管理工作。国务院电信主管部门、公安部门和其他有关机关依照本法和有关法律、行政法规的规定，在各自职责范围内负责网络安全保护和监督管理工作。本条对于关键信息基础设施运营者安全保护义务的监督管理机构做出了规定，即“1+X”模式，即国家网信部门负责统筹协调网络安全工作，国务院电信主管部门、公安部门及其他有关机关依照本法和有关法律、行政法规的规定，在各自职责范围内负责网络安全保护和监督管理工作。

《网络安全法》第五十九条规定，网络运营者不履行本法第二十一条、第二十五条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处一万元以上十万元以下罚款，对直接负责的主管人员处五千元以上五万元以下罚款；关键信息基础设施的运营者不履行本法第三十三条、第三十四条、第三十六条、第三十八条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。

以上规定集中体现了关键信息基础设施运营者不履行或者怠于履行关键信息基础设施运营者安全保护义务应该承担的法律责任。关键信息基础设施运营者是

网络安全的守门人,《网络安全法》第五十九条规定了网络运营者不履行本法第二十一条及二十五条规定的网络安全保护义务的处罚措施。

第一,责令改正。所谓责令改正是指行政主体责令违法行为人停止和纠正违法行为,以恢复原状,维持法定的秩序或者状态,具有事后救济性。对违法行为人给予行政处罚时,要同时责令行为人改正违法行为,不能以罚了事,让违法行为继续下去。“责令改正”在《网络安全法》的执法过程中有着重要作用,因此应该重视责令改正的具体操作。

第二,警告。国家对行政违法行为人的谴责和告诫,是国家对行为人违法行为所做的正式否定评价。警告是国家行政机关的正式意思表示,会对相对一方产生不利影响;对被处罚的关键信息基础设施运营者来说,警告主要是对当事人形成心理压力、不利的社会舆论环境。适用警告处罚的重要目的是,使被处罚人认识其行为的违法性和对社会的危害,纠正违法行为并不再继续违法。

第三,罚款。罚款是指行政机关对行政违法行为人强制收取一定数量金钱,剥夺一定财产权利的制裁方法。网络运营者不履行本法第二十一条、第二十五条规定的网络安全保护义务的,拒不改正或者导致危害网络安全等后果的,处一万元以上十万元以下罚款,对直接负责的主管人员处五千元以上五万元以下罚款;关键信息基础设施的运营者不履行本法第三十三条、第三十四条、第三十六条、第三十八条规定的网络安全保护义务的,由有关主管部门责令改正,给予警告;拒不改正或者导致危害网络安全等后果的,处十万元以上一百万元以下罚款,对直接负责的主管人员处一万元以上十万元以下罚款。本款的处罚有两个特色。第一,实行双罚制,对于网络运营者和直接负责的主管人员予以双罚。这一规定对于监督义务的履行具有更强的震慑作用。直接负责的主管人员是指该违法行为的决策者、事后予以支持和认可的领导、因疏忽大意或者放任不管而对单位违法行为应负有责任的领导。第二,对关键信息基础设施运营者比一般的网络运营者规定了更为严苛的违法责任。鉴于关键信息基础设施运营者对国家网络安全和社会正常秩序的运转具有不可替代的作用,因此应对其予以重点保护。

## 第 15 章

# 网络安全审查

网络安全审查制度是提升我国网络安全保障水平的重要制度设计，对实现关键信息基础设施网络产品和服务的安全性和可控性发挥着不可替代的基础性作用。自 2013 年全国人大代表、浪潮集团董事长孙丕恕向两会提交《建立信息安全审查制度》的提案之后，我国网络安全审查制度的法治化进程不断加快，包括《国家安全法》、《网络安全法》、《密码法（草案征求意见稿）》和《关键信息基础设施保护条例（征求意见稿）》在内的多部网络安全领域重要政策立法均对网络安全审查制度进行了明确规定。2017 年 5 月 2 日，中央网信办颁布了《网络产品和服务安全审查办法》（试行），作为《网络安全法》第三十五条的配套规定，审查办法进一步细化了网络安全审查制度的审查范围、审查内容和审查程序等核心内容，使网络安全审查制度进入到实质性的可操作层面。

### 第一节 《网络安全法》相关规定及释义

我国《网络安全法》第三十五条明确规定：关键信息基础设施的运营者采购网络产品和服务，可能影响国家安全的，应当通过国家网信部门会同国务院有关部门组织的国家安全审查。正式确立了我国的网络安全审查制度，成为提升我国

网络安全保障能力的重要举措。在全球范围内，我国并不是第一个建立网络安全审查制度的国家，但却是第一个建立具备法律理性的网络安全审查制度的国家。美国《2013 年合并与持续拨款法案》可以被认作全球第一部明确规定网络安全审查制度的立法，但该法案严重违背了“技术中立”原则和“非歧视”原则，专门针对中国的信息技术开展严格的安全审查要求<sup>①</sup>，被认为在全球范围内开创了极其糟糕的审查先例。在遭到包括美国信息技术产业界在内的多方抨击之后，尽管其后财年的《合并与持续拨款法案》在该事项上有所缓和，但仍然保留了对中国的歧视性规定<sup>②</sup>。由此可见，美国政府将网络安全审查作为赤裸裸的政策工具，该制度在法律理性方面缺乏必要的正当性基础。

而我国的网络安全审查制度则是在有效评估和考察了全球网络安全环境的基础上所进行的制度设计，是在充分认识信息技术“依赖性”和“风险性”的前提下所做出的路径选择。在过去的十几年中，“包括食物、供水、能源、通信、运输、医疗、金融、国防等在内的国家政务和军事基础设施对信息系统和网络的依赖度不断提高<sup>③</sup>。”这导致信息技术从仅供个人和组织使用的纯粹技术转变为国家的重要战略资源。作为信息技术利用的主要载体，网络产品和服务的安全性直接决定了国家网络安全保障能力的整体水平。然而遗憾的是，任何技术的馈赠都有其阴暗面，信息技术也存在其固有的脆弱性，即安全漏洞的普遍性。

安全漏洞是指在硬件、软件或协议的具体实现方面和安全策略方面存在的缺陷，使攻击者能够在未授权的情况下访问或破坏信息系统，是受限制的计算机、

① 该法案 516 条第 a 款规定，美国商务部、司法部、国家宇航局和国家科学基金会不得利用任何拨款采购信息技术系统，除非上述联邦机构负责人与联邦调查局或其他适当机构对网络间谍或破坏行为进行了风险评估，该风险包括由中国拥有、管理或资助的一个或多个机构所生产、制造或组装的信息技术系统有关的任何风险。第 b 款规定，上述联邦机构不得利用任何拨款采购根据第 a 款规定需要进行评估的信息技术系统，不得采购由中国拥有、管理或资助的一个或多个机构所生产、制造或组装的信息技术系统，除非第 a 款规定的评估机构的负责人决定并向众议院和参议院的拨款委员会报告，该系统采购符合美国的国家利益。

② 美国 2014 年的《合并与持续拨款法案》第 515 条第 a 款规定，美国商务部、司法部、国家宇航局和国家科学基金会不得利用任何拨款采购 NIST SP199 中规定的高影响（High-impact）或中度影响（Moderate-impact）的信息技术系统，除非上述联邦机构：（1）根据美国国家标准与技术研究院（National Institute of Standards and Technology, NIST）制定的有关标准进行供应链风险审查；（2）通过由联邦调查局或其他相关机构提供的威胁信息审查供应链风险；（3）联邦调查局或其他机构对与系统采购相关的网络间谍或破坏行为进行了风险评估，包括由美国政府认定实施了网络威胁的一个或多个组织生产、制造或组装的信息系统，包括但不限于由中国拥有、管理该法案或资助的组织。第 b 款规定，不得利用任何拨款采购经过第 a 款规定进行审查和评估的高影响或中度影响的信息技术系统，除非评估机构的负责人：（1）在咨询 NIST 和供应链风险管理专家之后，实施针对任何可识别风险的缓解策略；（2）决定该系统采购符合美国国家利益；（3）向众议院和参议院的拨款委员会报告该决定。

③ Recommendation on Critical Information Infrastructure Protection.OECD, 2008.

组件、应用程序或其他联机资源中不受保护的访问点。安全漏洞在网络产品和服务中广泛存在，在技术上被证明是无法避免的。这意味着网络产品和服务的部署必须正视由此引入的安全风险。2015 年 7 月，意大利黑客公司“Hacking Team”遭黑客攻击，泄露了 400GB 的内部资料。该事件引人注意的并不是资料泄露本身，而是资料披露出该公司向多国政府出售漏洞进行监控或入侵的事实，表明使用尚未披露的漏洞进行入侵和攻击在实践中非常有效<sup>①</sup>。

目前，大量的商业现货网络产品和服务被部署在关键信息基础设施中，直接影响相关信息和信息系统的的天性。随着信息技术供应全球化态势的加强，商业现货网络产品和服务的开发、生产和提供过程的安全性高度依赖供应链的完整性，“任何产品规格的变化，持续改进的措施，外包，内部网络重设，IT 更新，技术升级过程，供应商关系都会影响 IT 供应链的不确定性<sup>②</sup>。”IT 供应链的复杂程度导致商业现货网络产品和服务的安全性在很多情况下不可见，存在安全漏洞的网络产品和服务可能被恶意的内部和外部人员利用，实施网络攻击和破坏活动，严重威胁国家安全和社会稳定。为此，国家对重要领域中使用的网络产品和服务实施网络安全审查就变得十分必要，其能够识别与控制网络产品和服务中的安全风险，弥补传统检测认证无法涵盖产品和服务生命周期的弊端，有效提升国家网络安全的保障能力。

## 第二节 网络安全审查制度概述

目前，我国有多部政策立法明确规定了网络安全审查制度，除《网络安全法》外，早在 2013 年 9 月，工业和信息化部印发的《信息化发展规划》（工信部规〔2013〕362 号）第十二条“加强网络与信息安全保障体系建设”中就明确提出要确保基础信息网络和重要信息系统安全，其中的具体措施就包括“建立信息安全审查制度”。

① 马民虎，马宁．威胁态势感知视域下国家网络安全审查法律制度的塑造．

② Helen Peck. Drivers of supply chain vulnerability: an integrated framework[J].International Journal of Physical Distribution & Logistics Management, 2005 (4): 210-232.

其后，2014 年 5 月 22 日，国家互联网信息办公室发布公告称，我国将实行网络安全审查制度，明确将“国家安全和公共利益系统使用的重要技术产品和服务”作为审查对象；将“防止产品提供者非法控制、干扰、中断用户系统，非法收集、存储、处理和利用用户有关信息”作为审查目的；将“产品和服务的安全性和可控性”作为审查内容；同时规定“对不符合安全要求的产品和服务将不得在中国境内使用”。

2014 年 12 月 30 日，国家互联网信息办公室发布《关于加强党政部门云计算服务网络安全管理的意见》（中网办发文[2014]14 号），明确规定要建立云计算服务安全审查机制。

2015 年 7 月 1 日，第十二届全国人大常委会第十五次会议通过的新《国家安全法》建立了国家安全审查制度，其中明确将对网络信息技术产品和服务的安全审查作为国家安全审查制度的重要组成部分，为后续《网络安全法》中规定的国家网络安全审查制度奠定了坚实基础。

在《网络安全法》颁布之后，我国《密码法（草案征求意见稿）》第十八条和《关键信息基础设施保护条例（征求意见稿）》第三十一条均对关键信息基础设施网络产品和服务采购规定了网络安全审查的要求。《网络产品和服务安全审查办法（试行）》进一步对网络安全审查制度的实施进行了更为细化的规定。根据我国现有政策立法的相关规定，网络安全审查制度包含如下制度要素。

## 一、审查性质

根据相关立法的规定，我国目前实施的网络安全审查的性质仅限于国家安全审查，即只有在网络产品和服务影响或可能影响国家安全的情况下才实施网络安全审查。我国《国家安全法》第五十九条规定，国家建立国家安全审查和监管的制度和机制，对影响或者可能影响国家安全的外商投资、特定物项和关键技术、网络信息技术产品和服务、涉及国家安全事项的建设项目，以及其他重大事项和活动，进行国家安全审查，有效预防和化解国家安全风险。为此，我国的网络安全审查制度属于国家安全审查制度的一部分。国家安全审查制度的内容如图 15-1 所示。



图 15-1 国家安全审查制度的内容

可见，我国的网络安全审查制度有别于英美所建立的普遍性的安全审查活动，不是所有拟部署在关键领域的网络产品和服务均需要经过审查，这决定了我国的网络安全审查不是常态性的审查，也不会针对所有供应商进行开展，只有在采购活动可能影响国家安全的情况下才予以启动。根据《网络产品和服务安全审查办法（试行）》第十条规定，产品和服务是否影响国家安全由关键信息基础设施保护工作部门确定。

## 二、审查范围

国家网络安全审查的范围确定了实施安全审查活动的具体领域，根据我国《网络安全法》的规定，国家网络安全审查的范围限于关键信息基础设施，这与世界各国的做法保持一致。根据我国《网络安全法》第三十一条和《关键信息基础设施保护条例（征求意见稿）》第十八条的规定：我国的关键信息基础设施是指关系国家安全、国计民生，一旦数据泄露、遭到破坏或者丧失功能可能严重危害国家安全、公共利益的信息设施，包括但不限于提供公共通信、广播电视传输等服务的基础信息网络，能源、金融、交通、教育、科研、水利、工业制造、医疗卫生、社会保障、公用事业等领域和国家机关的重要信息系统，重要互联网应用系统等。具体包括以下内容。

（1）政府机关和能源、金融、交通、水利、卫生医疗、教育、社保、环境保护、公用事业等行业领域的单位。

（2）电信网、广播电视网、互联网等信息网络，以及提供云计算、大数据和其他大型公共信息网络服务的单位。

- (3) 国防科工、大型装备、化工、食品药品等行业领域科研生产单位。
- (4) 广播电台、电视台、通讯社等新闻单位。
- (5) 其他重点单位。

### 三、审查对象

网络安全审查制度的审查对象是指安全审查活动所作用的客体。我国《网络安全法》第三十五条规定：关键信息基础设施的运营者采购网络产品和服务，可能影响国家安全的，应当通过国家网信部门会同国务院有关部门组织的国家安全审查。《关于加强党政部门云计算服务网络安全管理的意见》第四条规定：中央网信办会同有关部门建立云计算服务安全审查机制，对为党政部门提供云计算服务的服务商，参照有关网络安全国家标准，组织第三方机构进行网络安全审查，重点审查云计算服务的安全性、可控性。《密码法（草案征求意见稿）》第十八条规定：国家对关键信息基础设施的密码应用安全性进行分类分级评估，按照国家安全审查的要求对影响或者可能影响国家安全的密码产品、密码相关服务和密码保障系统进行安全审查。为此，我国网络安全审查的对象为关键信息基础设施所采购的网络产品和服务，同时在一般性网络产品和服务之中特别规定了针对云计算服务和密码产品、密码相关服务和密码保障系统的安全审查。

在这里需要注意两个问题，其一是我国规定的网络安全审查对象未设定来源地标准，即针对国内和国外供应商均等同适用网络安全审查制度，不区分网络产品和服务的国别，不实行差别待遇；其二是尽管我国网络安全审查的对象明确为网络产品和服务，但已经考虑到信息技术供应链安全的重要意义，《网络产品和服务安全审查办法（征求意见稿）》第一条已然提出应当防范供应链安全风险，为此我国网络安全审查的对象事实上同时包括整个网络产品和服务供应链。

### 四、审查内容

网络安全审查制度的审查内容是指安全审查活动对何种事项开展审查。根据相关立法的规定，我国的网络安全审查将主要针对网络产品和服务的安全性和可控性。《网络产品和服务安全审查办法（试行）》第四条进一步将安全性和可控性



细化为 5 个方面，具体如下。

- (1) 产品和服务自身的安全风险，以及被非法控制、干扰和中断运行的风险。
- (2) 产品及关键部件生产、测试、交付、技术支持过程中的供应链安全风险。
- (3) 产品和服务提供者利用提供产品和服务的便利条件非法收集、存储、处理、使用用户相关信息的风险。
- (4) 产品和服务提供者利用用户对产品和服务的依赖，损害网络安全和用户利益的风险。
- (5) 其他可能危害国家安全的风险。

## 五、审查机构

《网络产品和服务安全审查办法（试行）》第五条、第六条、第七条和第九条规定了我国网络安全审查的审查机构，包括网络安全审查委员会、网络安全审查办公室、第三方机构和重点行业主管部门。其中，网络安全审查委员会是网络安全审查的领导机构，负责审议网络安全审查的重要政策，统一组织网络安全审查工作，协调网络安全审查相关重要问题。同时，网络安全审查委员会聘请相关专家组成网络安全审查专家委员会，在第三方评价基础上，对网络产品和服务的安全风险及其提供者的安全可信状况进行综合评估；网络安全审查办公室是实施机构，负责具体组织实施网络安全审查；第三方机构是评价机构，负责网络安全审查中的评价工作，为网络安全审查专家委员会提供第三方评价基础；重点行业主管部门是行业实施机构，负责组织和开展本行业和本领域内的网络安全审查工作。我国网络安全审查的审查机构如图 15-2 所示。

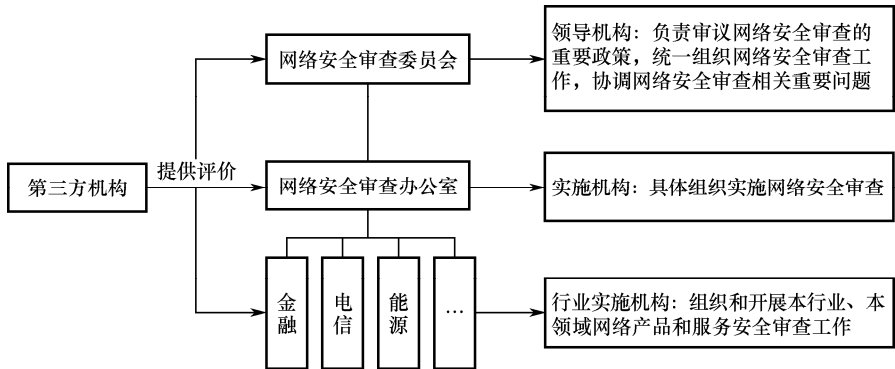


图 15-2 我国网络安全审查的审查机构

## 六、审查程序

《网络产品和服务安全审查办法（试行）》第八条规定，根据国家有关部门要求、全国性行业协会建议、市场反映等，网络安全审查办公室组织第三方机构、专家对网络产品和服务进行网络安全审查，并发布或在一定范围内通报审查结果，同时结合有关网络安全审查机构的相关规定进行分析。我国的网络安全审查的审查程序基本可以分为 6 个步骤，如图 15-3 所示。①由国家有关部门、全国性行业协会、市场其他主体等向网络安全审查办公室提出审查申请；②由网络安全审查办公室组织第三方机构和网络安全审查专家委员会准备审查，并向网络产品和服务供应商告知审查已经启动及相关事项；③由网络产品和服务供应商向第三方机构提交审查材料；④由第三方机构对审查材料进行评价，并将评价结果反馈给网络产品和服务供应商，同时提交网络安全审查专家委员会；⑤由网络安全审查专家委员会根据第三方评价，对网络产品和服务的安全风险及其提供者的安全可信状况进行综合评估，形成审查结论，并将该审查结论反馈给网络安全审查办公室；⑥由网络安全审查办公室将审查结果公布或在一定范围内通报。

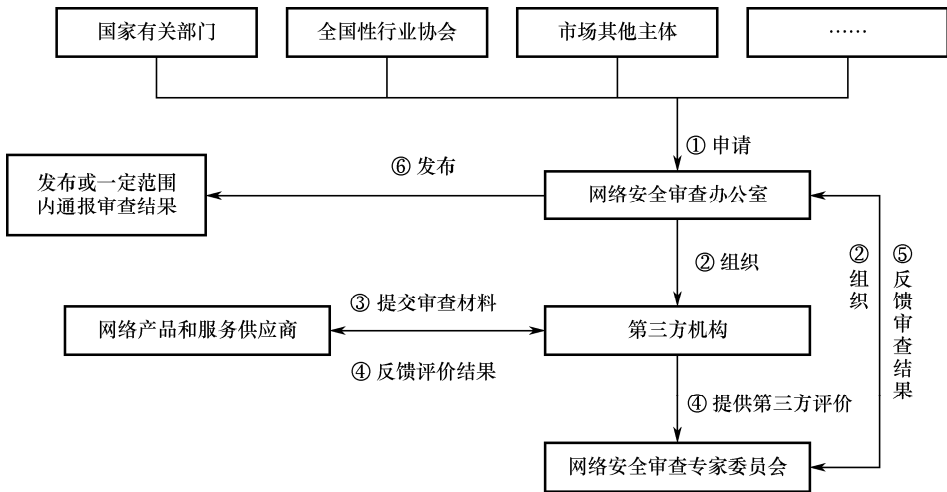


图 15-3 我国网络安全审查的审查程序

## 七、法律责任

根据我国《网络安全法》第六十五条的规定，关键信息基础设施的运营者在两种情况下将承担相应的法律责任，一是使用未经安全审查的网络产品和服务，二是使用安全审查未通过的网络产品或者服务。在关键信息基础设施网络运营者存在上述违法行为时，我国《网络安全法》采取了双罚制的处罚原则，对于关键信息基础设施的运营单位，由有关主管部门责令停止使用采购的网络产品和服务，并对单位处采购金额一倍以上十倍以下罚款；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

### 第三节 美英网络安全审查的相关实践

各国尽管鲜有直接规定网络安全审查的相关立法规定，但普遍对网络产品和服务在关键领域中的使用有严格的安全要求，起到了与我国网络安全审查制度类似的保障效果。近年来，随着全球网络安全态势的急剧恶化，网络产品和服务的安全性愈发引起了各国政府的高度重视，也开始出现了专门性的网络安全审查立法。综合来看，目前各国所广泛采用的网络安全审查重点涉及重要信息系统中的信息技术采购和云计算服务提供，此外还包括评估国家和政府机构网络安全能力的政策审查或弹性审查等，形成了包括技术审查、能力审查和弹性审查等多种模式的、完备的网络安全审查体系，为我国建立和完善网络安全审查制度提供了可资借鉴的蓝本。

#### 一、网络产品和服务采购安全审查

网络产品和服务采购安全审查是各国类似制度的核心内容，通过对供应商实施有别于传统测评认证的安全审查，进一步验证在重要领域部署的网络产品和服务的安全性，保障信息与信息系统的完整性、保密性和可用性。

## （一）美国政府信息技术采购安全审查

政府信息技术采购历来是美国政府管控的重点，在国家信息保障的总体要求下，结合政府信息技术采购和认证认可的具体实践，美国国家安全局（National Security Agency, NSA）和国家技术标准研究院（NIST）共同开发并实施了国家信息保障合作（National Information Assurance Partnership, NIAP）计划，审查国家安全系统<sup>①</sup>中使用的商业现货网络产品和服务，确保其符合美国相关政策立法中确定的安全性标准。

早在2000年7月，美国国家安全通信和信息系统安全委员会（National Security Telecommunications and Information Systems Security Committee, NSTISSC）<sup>②</sup>发布了“国家信息保障采购政策”（National Information Assurance Acquisition Policy）<sup>③</sup>，该政策规定，自2001年7月1日起，所有国家安全信息系统中采购的信息技术产品必须满足评估和验证要求，首先必须满足互认的国际信息安全技术评估通用标准的安全要求；其次必须满足NSA、NIST和NIAP的评估认证程序；或满足NIST联邦信息处理标准（Federal Information Processing Standards, FIPS）的认证程序。相关的评估认证工作由可信的商业实验室或NIST实施，自2002年6月1日起，所有国家安全信息系统采购的信息技术产品只能限于通过上述评估认证的产品，同时必须接受NSA的评估或符合NSA批准的流程。关键基础设施保护第63号总统令规定的非国家安全系统也可以考虑适用上述评估和认证要求，这些信息系统尽管仅涉及非保密性信息，但其对于实现特定功能意义重大。

2013年6月10日，美国国家安全系统委员会（Committee on National Security Systems, CNSS）发布了第11号政策《管理信息保障和实现信息保障的信息技术

① 根据1994年美国《国家安全通信和信息系统认证认可政策》的规定，国家安全系统（NSS）是指：任何由政府机构、政府机构合同商或代表机构履行职责的其他组织使用或运维的下列信息系统（包括通信系统）：

（1）其功能、运行和使用涉及情报、与国家安全相关的密码技术、军事事项，或其包括武器或武器系统的设备；（2）涉及由行政命令或国会法案特别授权永久保护的信息系统。

② 美国国家安全通信和信息系统安全委员会是根据美国1990年的第42号国家安全指令建立的国家安全通信和信息系统安全管理机构，主要负责制定和颁布适用于国家安全通信和信息系统的国家安全政策。

③ NSTISSP（National Security Telecommunications and Information Systems Security Policy）No. 11: National Information Assurance Acquisition Policy，有学者将该政策译为“国家信息安全采购政策”，但本报告认为，信息安全有固定表达，应为Information Security，而Information Assurance在美国信息安全相关标准中有明确定义，实为信息保障（Information Assurance, IA）。根据NSTISSC 2009发布的第4009号指令《国家信息系统安全术语》，信息保障是指“通过实现可用性、完整性、认证性、保密性和抗抵赖性保护信息和信息系统的信息操作，包括提供结合保护、检测和反应的信息系统恢复能力”。

产品采购的国家政策》，该政策重申了 NSTISSP 第 11 号政策的采购要求，强调所有国家安全系统采购的信息保障或实现信息保障的信息技术商业现货产品必须满足 NIAP 和 NSA 的评估和认证要求，加密产品必须满足 FIPS 中涉及密码的验证项目要求。CNSS 的采购政策更进一步明确了国家安全系统信息技术产品采购中各方主体的责任，使得基于信息技术产品安全评估和认证的安全审查工作更具实践性和可操作性。

为了满足 CNSS 第 11 号政策的要求，NSA 与 NIST 共同开发和实施了 NIAP。根据 NIAP 建立的审查框架，意欲向美国联邦机构运维的国家安全系统提供信息技术产品的供应商首先需要经过 NIST 或 NIAP 授权或同意的通用标准测试实验室（Common Criteria Testing Laboratory, CCEL）对信息技术的安全性进行验证，提交 NIAP 同意使用的保护简介（Protection Profile, PP）<sup>①</sup>和安全目标草案<sup>②</sup>。CCEL 对供应商的信息技术产品依据提交的材料进行分析和测试后将验证报告提交给 NIAP 进行审查，符合安全要求后，NIAP 向供应商颁发 NIAP 认证证书，向 CCEL 和供应商反馈安全性验证报告，保障活动报告，管理指南和最终的安全目标。同时向社会发布产品遵从清单和认证产品清单，供联邦政府机构信息技术采购参考和选择。

## （二）英国中央政府信息技术采购安全审查

长久以来，英国对于政府机构的信息技术利用始终秉承中立和开放态度，除国防供应系统之外，一般允许各政府机构自由采购信息技术产品和服务，但是必须建立在统一规范的基础上。2014 年 9 月 25 日，英国内阁办公室颁布了 09/14 号行动公告《采购政策公告——使用网络要素体系认证》（Procurement Policy Note—Use of Cyber Essentials Scheme certification, PPN），该公告于 2014 年 10 月 1 日生效。在该份公告中，英国内阁办公室鼓励政府机构广泛采用网络要素认证体系，其中，强制要求在 2014 年 10 月 1 日以后参与处理个人信息和提供特定信息通信技术产品和服务的供应商必须适用网络要素体系，开启了真正意义上政府信息技术采购安全审查的时代。

英国《网络要素体系》分为两个基础部分，包括保障框架和安全要求。其中

① 保护简介是指为符合特殊用户需求而强制特定类别信息技术产品需要满足的安全要求。

② 安全目标是指需要经过验证的信息技术产品安全功能的规范，也被用于描述产品相关的运行环境。

保障框架可以视为供应商安全认证的程序规定，提供了两个阶段的认证要求，即 Cyber Essentials 和 Cyber Essentials Plus，供应商可以根据自身的网络安全风险水平和成本考虑，选择适合安全目标的认证过程。根据网络要素体系保障框架的规定，Cyber Essentials 属于供应商自我评估的验证过程，这一过程中的认证活动提供了基础性的可信水平，确认供应商实施了正确的风险控制措施，认证范围只包括网络边界、位置和管理控制。因此，Cyber Essentials 只适用于那些被认为处于低风险，或只要求基本技术保护措施的信息系统。当供应商验证自身符合有关网络要素体系安全要求时，可以向认证机构申请认证。在满足 Cyber Essentials 的基础上，Cyber Essentials Plus 提供了一种更高水平的认证过程，属于独立性测试过程，用于验证供应商的安全控制措施是否充分，该验证通常基于脆弱性测试，涵盖供应商内外部的所有信息系统。但是基于网络安全要素的认证“只能作为供应商弱化风险能力的简单印象，并不能反映其风险控制的可持续性<sup>①</sup>”。为此，供应商通常需要每年进行重新认证，或为满足特定采购需要而在必要时进行认证。

在英国政府信息技术采购安全审查框架中有两项内容引起了我们的特别注意：其一，英国内阁办公室定义的中央政府机构的范围非常广泛，包括非部长级部门（Non-Ministerial）、行政机构（Executive Agencies）和非部门化的公共实体（Non-Departmental Public Bodies），上述机构需要强制性地适用 PPN 的相关规定，而地方政府和公共部门可以选择适用 PPN 中的相关规定；其二，考虑到信息技术的多样性和部门信息系统的敏感性，同时避免重复审查对政府部门和供应商产生的负担，供应商在特定情况下可以豁免适用《网络要素体系》的安全要求，这些情况包括政务云服务（G-Cloud）<sup>②</sup>、数字服务框架（Distributed Service Framework, DSF）<sup>③</sup>、公共部门网络（Public Sector Network, PSN）<sup>④</sup>、身份认证框架（Identity Authentication Framework, IDAF）<sup>⑤</sup>、辅助性的数字服务（Auxiliary Digital, AD）<sup>⑥</sup>。

① HM Government. Cyber Essentials Scheme Assurance Framework[R].UK, 2015.

② 英国政务云服务采购需要满足《政府云服务安全原则》的相关审查要求。

③ 在英国，DSF 的供应商通常已经通过技术性和商业性评估。

④ 英国的 PSN 服务供应商目前需要经过依据网络安全标准的认可活动，但是 PPN 同样考虑将来依据政府网络安全原则对 PSN 进行安全评估。

⑤ 英国要求为国家和地方政府机构、主要互联网公司、在线零售商、银行和其他公共服务机构提供在线身份保障服务的供应商应当围绕身份验证和用户名/口令错误等事项解决商业和安全诉求，避免身份欺诈和个人数据侵犯。

⑥ AD 主要用于支持不能独立使用在线服务的人员，其安全要求目前由英国政府数字服务（Government Digital Service, GDS）进行规定。

此外，向英国国防部（Ministry of Defence, MoD）提供服务的供应商也豁免适用《网络要素体系》。

## 二、云服务安全审查

严格来讲，云服务安全审查同样属于网络产品和服务采购安全审查，需要满足国家关于网络产品和服务采购安全审查的统一规定，但鉴于云服务分布式存储和提供的特殊性，美英通常对云服务进行独立审查。

### （一）美国 FedRAMP 云服务安全审查

美国技术和标准研究院、通用服务管理局、国防部和国土安全部共同开发了《联邦风险和授权管理程序》（Federal Risk and Authorization Management Program, FedRAMP）进行政府云安全审查，针对云服务开展标准化的安全评估、授权和持续性监控，其目的在于确保政务云系统具有充分的安全保障，降低在云风险管理方面的成本，提高政府信息系统和服务采购的效率。美国预算管理办公室（Office of Management and Budget, OMB）2011 年 12 月 8 日的政策备忘录中强制要求，2012 年 6 月以后政府采购的云服务必须满足 FedRAMP 的安全要求，现存的已经采购的云服务到 2014 年 6 月前必须通过 FedRAMP 安全审查。

FedRAMP 采取了较为灵活的云安全审查方式以提高审查效率，提供三种模式<sup>①</sup>供云服务商选择，其审查主体和程序略有区别，但具有同等的审查效力。

但是无论选择哪种审查模式，FedRAMP 均需要满足《FedRAMP 审查和批准标准化操作程序》（FedRAMP Review and Approve Standard Operating Procedure）所规定的审查程序。根据该程序，任何类型的 FedRAMP 云安全审查均包括四个阶段，第一是准备和申请阶段，在该阶段由云服务商准备待审查的资料，选择审查机构和提起审查申请；第二是接受审查阶段，由审查机构根据云服务商提交的审查资料的有效性和充分性决定是否接受审查；第三是细节审查阶段，该阶段是 FedRAMP 审查的核心阶段，在审查机构同意接受审查之后，对云服务商提交的审

---

<sup>①</sup> 三种模式即联合授权委员会模式、联邦机构授权模式和自行审查模式。

查材料进行细节性的安全验证；第四是批准阶段，在通过审查机构的安全审查之后，云服务商被批准向政府机构提供相关的云服务，并被列入安全清单。

在实体内容方面，FedRAMP 建立完备的安全审查框架（见表 15-1），列明了云服务商需要满足的安全控制要求，其主要依据 NIST SP 800-53 和 SP 800-37 这两个基础性标准，分为文档化、评估、授权和监控 4 个基础管理域。

表 15-1 FedRAMP 审查框架

安全控制要求	描述
1. 文档化	
1.1 信息系统分类	云服务商应按照 PUB 199 的要求对信息和信息系统进行分类，以决定哪类数据会（或可能）对系统产生决定性影响。分类的方法参照 SP 800-60 中关于信息映射类型和信息系统安全类别的指南。FedRAMP 仅支持低影响度或中影响度级别系统的安全评估
1.2 选择安全控制措施	云服务商需要在《FedRAMP 系统安全计划模板》(FedRAMP System Security Plan Template) 规定的安全控制基线中选择云服务需要采用的安全控制措施，该基线包含 17 类安全控制措施，构成了满足 FedRAMP 审查的最低安全控制要求
1.3 实施安全控制措施	云服务商选择 FedRAMP 安全控制基准之后便需要落实与相关影响级别相符的安全控制措施。对于大多数云服务商而言，许多控制措施事实上已经进行了实施，但需要在 FedRAMP 模板中进行详细描述。有些控制措施可能需要云服务实现新的功能，有些控制措施可能需要重构现有的实施方式。在这一点上，FedRAMP 考虑到云服务商的系统之间可能存在差异，允许在实施补偿控制或可选择的实施措施之间有一定的灵活性，但安全控制的目的必须得到满足。云服务商可以提供替代性的实施措施，但需要证明满足了安全控制要求
2. 评估	
2.1 第三方评估机构	云服务商进行 FedRAMP 安全审查应当选择经过认证的独立第三方评估机构
2.2 非认证评估机构	FedRAMP 并不强制要求云服务商选择经过 FedRAMP 认证的评估机构，如果云服务商选择由非认证的评估机构对云服务的安全性进行验证，那么需要对该评估机构的独立性和技术资格进行证明
2.3 完整的安全评估计划	评估机构需要根据 FedRAMP 的审查框架编制完整的评估计划，该计划应包括评估范围内的所有资产，如硬件、软件和物理设施的组件，安全性验证的方法，并证明评估机构使用了 FedRAMP 的相关安全评估方法
2.4 评估程序	对云服务商选择的安全控制措施，第三方评估机构应当建立评估程序，该程序应当能够充分评估云服务提供商控制措施实施的有效性，以及任何实施阶段可能出现的风险
2.5 评估活动	评估机构对云服务商的系统进行与评估程序相一致的安全性验证，云服务商在评估期间应当尽可能锁定系统以便于修复评估发现的风险



续表

安全控制要求	描述
3. 授权	
3.1 风险分析	完成安全评估之后, 评估机构需要形成评估报告并在其中呈现对风险分析和结果的判断。安全评估报告包含评估过程中发现的漏洞、威胁和风险的相关信息, 包括对减少云服务商脆弱性的建议。安全评估报告首先应送至云服务商, 以明确是否存在第三方评估机构在生成安全评估报告时未考虑到的因素、误报情况或其他信息。授权官员将对安全评估报告进行分析, 并确定云服务商系统的整体安全性
3.2 行动计划与时间表	云服务商针对安全评估报告中提出的特定缺陷编制行动计划与时间表。云服务商需要证明其针对发现的每个安全缺陷都有合适的改进计划, 其中包含人事、资源、进度等因素
3.3 授权安全文档的提交	云服务商必须为安全审查整理出最终的授权安全文档, 应包含审查活动生成和引用的所有文件, 安全评估中所有的计划和相关结果, 安全评估报告, 以及行动计划与时间表。授权官员将审查整个授权安全文档, 并在风险分析的基础上做出是否对系统授权的决定。根据信息自由法案的规定, 所有已提交的授权安全文档必须在封面和封底页做出适当的敏感标记
3.4 授权书	一旦授权官员对云服务商做出了基于风险分析的授权决定, 将向云服务商发放授权证书。授权官员需要向联邦风险和授权管理程序项目管理办公室提供这些证书的副本, 以便于联邦风险和授权管理程序项目管理办公室能够对联邦机构的云服务使用情况进行核查
3.5 撤销授权	被授权的云服务商应实施持续性监控, 以持续满足 FedRAMP 的各项要求, 并将风险维持在低、中安全影响等级内。如果云服务商不能符合 FedRAMP 持续性监控的要求, 维持其风险状态, 授权官员可以选择撤销该云服务商的授权, 并通知联邦风险和授权管理程序项目管理办公室。联邦风险和授权管理程序项目管理办公室将把云服务商的授权变化通知给利益相关方
4. 监控	
4.1 运营可视性	为了实现运营可视性, 云服务商需要定期提交控制实施情况说明, 每年还需要对云服务的安全性进行重新评估, 并向使用服务的机构和联邦风险和授权管理程序项目管理办公室提交结果。年度评估应当按照《FedRAMP 年度评估办法》的规定, 以初始授权同样的方式进行
4.2 变化控制	云服务商可能在系统配置管理计划程序之内, 对系统进行阶段性改变。云服务商必须对任何会对联邦风险和授权管理程序要求产生严重影响的变化或变化计划进行报告。云服务商必须将任何配置管理计划之外的系统变化通知授权官员, 以确定该变更是否达到显著变化的程度
4.3 应急响应	云服务多租户共享资源的模式决定了安全事故可能对使用云服务的多个联邦机构产生影响, 云服务商应当编制相应的应急响应计划。OMB M-07-16 和 NIST SP 800-61 均对应急响应计划有相关要求。根据安全事故的严重性与其所造成的后果, 以及其对云服务商安全性所造成的影响程度, 授权官员可以启动对云服务商的授权审查, 未进行事故报告也有可能导致云服务商接受授权审查

## （二）英国 G-Cloud 服务云安全审查

英国实行统一的云服务采购公共服务平台 G-Cloud，云服务提供方和采购方均可在该平台注册，建立便捷化的公私采购系统。G-Cloud 包含两部分主要内容，一是框架协议，公共部门可以通过该框架协议直接采购供应商的云服务，而不需要经过全面招标，简化了采购流程；二是建立了类似在线商店的采购库“数字市场”（Digital Marketplace），公共部门可以在该市场中选择满足 G-Cloud 安全要求的云服务。可见，G-Cloud 事实上扮演了第三方交易平台的角色，主要目的在于促进云产业的快速发展，便利政府云服务的采购流程。

英国在普及政府云应用的过程中同样十分重视云服务中分布式计算模式可能对政务数据安全产生的威胁。2014 年，英国国家网络安全中心（National Cyber Security Centre，CESG）和内阁办公室开发了一系列云安全原则，用于验证云服务的安全性，这些安全原则同样被用于向政府提供云服务的供应商安全审查中。根据英国 9/14 号行动公告，向政府提供云服务的安全审查不适用《网络要素体系》的安全控制要求，而需要依据政府云服务安全原则审查云服务的安全性。到目前为止，CESG 和内阁办公室一共发布了 14 项云服务安全原则，供应商向政府部门提供云服务时，由第三方认证机构和授权官员对供应商对云服务安全原则的遵从情况进行审查和验证，供应商需要在自我声明中阐述自身所实施的安全控制措施，并以合同的方式列明这些安全控制要求，在服务提供和维护的过程中履行信息保障的相关要求。

## 三、网络安全能力审查

除针对网络产品和服务安全以外，美英极为关注自身网络安全能力的建设，开展了专门针对国家网络安全能力或网络安全弹性的审查活动，特别是在发生重大国际网络安全事件之后，会针对该次事件审查本国是否具备抵御类似安全事件的能力。例如 2017 年 1 月 6 日，美国情报委员会发布了针对 2016 年美国大选遭到俄罗斯黑客攻击的调查报告<sup>①</sup>。两天之后，英国国家安全战略联合委员会即宣布

---

<sup>①</sup> Background to “Assessing Russian Activities and Intentions in Recent US Elections”: The Analytic Process and Cyber Incident Attribution, [https://www.dni.gov/files/documents/ICA\\_2017\\_01.pdf](https://www.dni.gov/files/documents/ICA_2017_01.pdf).

开始进行国家网络安全审查,以确保英国不会遭到类似的网络攻击<sup>①</sup>。目前,我国的网络安全审查制度尚未关注相关内容,但美英对于网络安全能力的审查对综合提升国家网络安全水平,落实国家网络安全保障要求起到了至关重要的作用,其相关做法值得我国吸收和借鉴。

### (一) 美国网络安全弹性审查

美国比较著名的网络安全弹性审查主要包括国家网络安全审查(Nationwide Cyber Security Review, NCSR)和网络弹性审查(Cyber Resilience Review, CRR)。NCSR是由国土安全部联合网络安全多状态信息共享和分析中心(MS-ISAC)、国家首席信息安全官协会(NASCIO)和国家郡县协会(NACO)实施的国家网络安全审查,该审查是面向所有联邦和地方政府机构开展的自愿性自评估审查,主要内容是审查各机构对2014年NIST发布的网络安全框架的遵从和落实情况,于每年10月的“网络安全意识月”期间予以开展。

CRR是另一项由国土安全部主导的自愿性国家网络安全态势审查,同样属于网络安全的非技术性审查,该审查主要用于评估各政府机构和关键基础设施部门的网络安全能力和运维弹性。CRR由美国网络安全评估项目(Cyber Security Evaluation Program, CSEP)负责管理,由工业控制系统网络应急响应小组(Industrial Control Systems Cyber Emergency Response Team, ICS-CERT)负责提供网络安全评估工具。CRR所采用的原则和实践标准与NIST网络安全框架保持一致。CRR主要审查各政府机构和关键基础设施部门的资产管理、控制管理、配置和变更管理、漏洞管理、安全事件管理、服务持续性管理、风险管理、外部依赖性管理、培训和意识、态势感知这十方面的相关内容。

### (二) 英国网络安全能力审查

2015年,英国政府发起了一项针对国家网络安全能力的安全审查,该项审查由全球网络安全能力中心(Global Cyber Security Capacity Centre, GCSCC)负责实施,包括政府机构、学界、犯罪司法和执法机构、立法和政策制定机构、应急

---

<sup>①</sup> UK to review its cyber security after US election hacks. <https://www.cnet.com/news/uk-reviewing-its-cyber-security-after-us-election-hacks>.

响应中心、私有部门、通信技术公司、金融机构和网络武装力量在内的多方主体参与其中。为了便利审查工作，GCSCC 建立了统一的网络安全能力成熟度模型逐一审查英国的相关情况，该模型包含五个主要要素，分别为：网络安全政策和战略，网络安全文化和社会，网络安全教育、培训和技能，网络安全立法和规范体系，网络安全标准、商业模式和技术。

## 第四节 我国网络安全审查制度法规遵从框架及建议

从目前我国网络安全审查制度的相关规定来看，已经包含了审查性质、审查范围、审查对象、审查内容、审查机构和审查程序等基础性法律要件，初步建立了制度框架。但从可实施性和指引性的角度判断，现有规定仍然不能对关键信息基础设施的运营者以及网络产品和服务的供应商提供必要的法规遵从指引，即相关主体无法通过现有规定确切知悉自身为满足法规遵从所应实施的改善措施，也无法通过现有规定评估自身是否满足《网络安全法》的强制性要求，是否可以通过安全审查。现有问题的核心在于审查内容的模糊性和标准依据的缺失。为此，我们可以借鉴国外在网络产品和服务安全性控制方面的实践经验，初步提出引导性的遵从建议，供关键信息基础设施运营者及网络产品和服务的供应商判断自身对于《网络安全法》的遵从程度，进而实施相应的改善措施。

### 一、网络产品和服务安全性遵从

美国 1996 年的《克林格—科恩》法案废除了由 1949 年《联邦资产与管理服务法》所确立的总务署（The Administrator of General Services）集中授权采购的方式，由各联邦机构具体负责信息技术的采购事项。为此，各联邦机构均制定和实施了符合自身利益的信息技术采购政策，其中以美国内政部（Department of the Interior, DOI）的信息技术采购要求最为完备。根据 DOI 第 375 号部门手册的要求，所有 DOI 部门在信息技术采购中的所有采购招标文件必须附加信息安全要求。

2005 年 DOI 专门发布了《信息技术采购安全要求指南》，详细列举了供应商在 DOI 信息技术产品和服务采购活动中所应满足的安全性要求（见表 15-2），可以将其作为我国网络安全审查法规遵从的参照系。

表 15-2 DOI 信息技术采购安全审查框架

商业现货供应（Commercial Off-the-Shelf）软硬件	
针对商业现货供应软硬件，DOI 仅针对产品质量进行安全审查，要求所有的软硬件不存在病毒、木马、蠕虫、间谍程序等恶意代码，并且供应商必须通过合同的方式将该安全保障确定化	
开发和维持客户端应用的服务和外包类信息技术服务或在线支持服务	
1.背景审查	背景审查，该项审查仅针对可能访问 DOI 信息资源的供应商人员，并不包括供应商本身。背景审查遵循的基本原则是，针对供应商雇员背景审查的水平应当与处于类似工作职位的联邦政府雇员相一致。根据实际情况，DOI 可能附加国家机构检查和问询的要求。背景审查的内容可能涉及人员工作、教育、居住、执法、法庭记录、公共记录、信用记录等众多内容，而其记录年限根据不同的审查类别有所区别 <sup>①</sup> 。而且供应商在访问 DOI 信息之前，必须与之签订非披露的保密协议
2.培训审查	由于 DOI 强制要求信息技术采购中涉及的所有供应商雇员，特别是那些能够访问 DOI 信息资源的供应商雇员必须在提供服务之前接受联邦信息系统安全意识培训（FISSA），该培训内容会定期更新，以适应信息技术快速发展所产生的风险因素变动影响
3.位置审查	根据 DOI 的要求，为了充分保障政务敏感信息的安全性，供应商提供的软件开发和外包服务必须位于美国境内。如果该业务确需在境外完成，供应商则需要提供可接受的安全计划以降低可能产生的通信、控制、数据保护或其他安全风险
4.系统开发完整性审查	DOI 要求供应商应当满足 NIST SP 800-64 和 DOI 系统开发生命周期（SDLC）完整性安全指南的相关要求。其中，NIST SP 800-64 名为《系统开发生命周期中的安全考虑》，是联邦范围内 SDLC 信息安全符合度的重要参考
5.价值评估审查	这里的价值评估主要针对信息系统相关资产的敏感度和风险评估。DOI 要求信息技术采购中的供应商必须使用《DOI 资产价值评估指南》 <sup>②</sup> 对信息系统的目标影响、数据敏感度、风险水平和机构的关键性进行评估，并评估该系统将作为主要应用、次要应用还是一般性支持系统予以开发和部署
6.独立性验证审查	独立性验证审查活动主要针对软件的升级活动实施审查，DOI 要求所有的软件在进入生产环节之前必须进行软件升级的独立性验证（IV&V），该验证过程由独立的第三方机构完成。IV&V 可以被认作一种审查方法，其目的在于证明信息技术开发和采购符合安全要求，并保证信息技术产品和服务进行部署以后，能够按照预期的方式和环境进行使用。同时，DOI 并没有强制要求 IV&V 必须由政府采购方主导，供应商可以自主进行该项验证。因此在签订采购合同之前，供应商应当明确地表明是否由己方申请和完成 IV&V

① DM441, chapter4, 4.15.  
② DOI Asset Valuation Guide.

续表

7.认证认可审查	认证认可审查主要针对根据《DOI 资产价值评估指南》而确立的主要应用和一般性支持系统，DOI 要求该系统在生产之前必须通过认证认可，并且每三年需要重新认可，在发生安全环境的重大变化时，也需要进行重新认可。DOI 要求供应商需要满足的信息安全标准非常复杂，包括《联邦信息系统安全计划开发指南》 <sup>①</sup> 、《风险评估实施指南》 <sup>②</sup> 、《联邦信息系统风险管理框架应用指南》 <sup>③</sup> 、《联邦信息系统和组织安全和隐私控制评估》 <sup>④</sup> 、《信息和信息系统安全分类指南》 <sup>⑤</sup> 、《联邦信息和信息系统安全分类标准》 <sup>⑥</sup> 、《联邦信息和信息系统最低安全要求》 <sup>⑦</sup> ，同时，DOI 内部的指南和标准也被作为重要参照，例如 DOI《安全测试和评估指南》、《隐私影响评估》等
8.漏洞分析审查	DOI 要求信息技术采购的供应商必须部署漏洞分析工具每月进行漏洞扫描，在所有的高风险系统中，任何源自互联网的系统访问必须经过渗透测试。同时，政府信息技术采购方拥有利用政府雇员和其他第三方对系统进行漏洞骚扰的权力。供应商必须采取适当的措施修正或减轻在测试中发现的脆弱性
9.安全控制审查	DOI 要求所有信息技术采购中的供应商满足 NIST SP800-53 和 NIST FIPS200 中规定的安全控制要求，供应商采取的安全控制措施应当与信息 and 信息系统的敏感度或关键度相一致。在 NIST FIP200 中，NIST 给出了根据信息和信息系统影响水平选择安全控制措施的方法，其将联邦信息系统分为低影响、中等影响和高影响三个级别，分别要求上述信息系统必须满足 NIST SP800-53 所确定的低基线、中等基线和高基线的最低安全保障要求

二、云计算服务安全审查

我国目前已经开展了云计算服务安全审查，2016 年 9 月，浪潮软件集团有限公司的“济南政务云平台”、曙光云计算技术有限公司的“成都电子政务云平台（二期）”和阿里云计算有限公司的“阿里云电子政务云平台”3 项云服务通过网络安全审查。根据《关于加强党政部门云计算服务网络安全管理的意见》的规定，为党政

① NIST SP 800-18:《Guide for Developing Security Plans for Federal Information Systems》。  
② NIST SP 800-30:《Guide for Conducting Risk Assessments》。  
③ NIST SP 800-37:《Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach》。  
④ NIST SP 800-53:《Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans》。  
⑤ NIST SP 800-60:《Guide for Mapping Types of Information and Information Systems to Security Categories》。  
⑥ NIST FIPS199:《Standards for Security Categorization of Federal Information and Information Systems》。  
⑦ NIST FIPS200:《Minimum Security Requirements for Federal Information and Information Systems》。

部门提供服务的云计算服务平台、数据中心等要设在境内，这成为我国云服务安全审查的基本遵从要求，但在云服务的安全性方面，目前缺乏明确的遵从指引。

2014 年，英国国家网络安全中心（National Cyber Security Centre，NCSC）和内阁办公室开发了 14 项云安全原则（见表 15-3），用于验证云服务的安全性，这些安全原则同样被用于向政府提供云服务的供应商安全审查中。这些云服务安全原则及其安全控制目标具有相当程度的普适性，可以成为我国云服务商进行法规遵从的参考蓝本。

表 15-3 英国云服务安全核心原则与目标

云服务安全原则	安全控制目标
原则 1：数据传输安全保护	用户的数据传输网络应当进行充分保护，防止数据篡改和窃听，云服务商应当实施网络保护，防止攻击者访问或拦截数据；实施加密保护，防止攻击者读取数据。实现用户终端设备与服务器之间的数据传输保护；实现服务内部的数据传输保护；实现服务与其他服务之间的数据传输保护
原则 2：资产保护与弹性	用户数据及相关资产的存储和处理应当防止物理篡改、丢失、损坏和拦截。保证用户知悉其数据将在哪里进行存储、处理和管理，以及对于当地法律遵从的影响；确保物理设施采取了充足的安全保护措施，实现服务持续性提供；静态数据使用受保护的媒体进行存储，防止未经授权的访问；服务设备在服务生命周期终止后，应当进行必要的安全处理，防止对服务和用户数据的安全性造成减损；应当保证服务的可用性，包括容灾能力和恢复能力
原则 3：用户隔离	用户隔离可以防止恶意用户或存在安全隐患的用户影响服务或其他用户数据的安全。保证用户知悉与其共享服务和平台的其他用户的情况；实施有效的用户数据和服务隔离措施；对于用户数据的管理也应当实施隔离措施
原则 4：管理框架	云服务商应当实施安全的管理框架，包括清晰定义的安全管理人员、文档化的安全管理政策框架、信息安全风险报告机制、识别和确保服务商的法律遵从性
原则 5：操作安全	云服务商应当实施操作安全保护，包括如下基本内容：（1）配置和变更管理，云服务（包括硬件和软件）的状态、位置和配置应当在服务生命周期中予以跟踪；对云服务的变更应当进行安全影响评估，具体变更应当进行跟踪和管理。（2）漏洞管理，云服务商对于可能影响服务安全性的漏洞进行评估、监控，并采取缓解措施。（3）保护性监控，采取可疑活动的识别和分析措施，有效分析潜在的恶意活动迹象。（4）安全事件管理，实施有效的实践识别、响应和恢复措施，并建立及时的事件报告制度
原则 6：个人安全	用户基于安全考虑，应当可以选择能够访问用户数据或影响云服务的云服务商雇员，云服务商的雇员应当保证可信
原则 7：安全开发	云服务的设计和开发应当识别和降低安全威胁，相关的威胁应当在设计和开发过程中进行识别和审查，符合有关安全设计、编程、测试和开发的最佳实践，在开发、测试和部署环节实施必要的配置管理

续表

云服务安全原则	安全控制目标
原则 8：供应链安全管理	云服务商应当确保其供应链满足所有的安全原则，保证用户知悉供应链的信息共享模式、第三方采购流程、供应链管理安全要求
原则 9：用户安全管理	云服务商应当向用户提供帮助其进行安全管理的工具，确保只有经过授权的人员可以访问管理平台
原则 10：认证和授权	用户和云服务商均应当经过认证和授权才能访问云服务，云服务商应当实施必要的认证和授权控制措施
原则 11：外部接口保护	云服务商应当对所有的外部接口或非可信接口进行识别并提供必要的保护措施，防止网络攻击
原则 12：安全服务管理	云服务的安全水平取决于云服务商管理系统的安全水平，云服务商进行服务操作管理的方法和措施应当识别和降低安全威胁
原则 13：用户审计信息	云服务商应当保证向用户提供审计信息，使用户能够监控其服务和数据的访问情况，供用户发现和应对对其服务和数据进行的恶意使用或其他威胁
原则 14：用户服务安全使用	云服务商应当保证用户知悉能够选择的服务配置和安全措施，保证用户了解进行数据处理、使用的安全要求，为用户提供安全管理和使用云服务的必要培训

我国发布的《信息安全技术 云计算服务安全能力要求》(GB/T 31168—2014)标准中同样提出了十类安全要求(见表 15-4)，成为在我国开展云计算服务的安全基线，也可以成为在云服务安全审查中的审查标准。

表 15-4 我国云服务安全要求

云服务安全要求	安全控制目标
安全要求 1：系统开发与供应链安全	云服务商应在开发云计算平台时对其提供充分保护，为其配置足够的资源，并充分考虑信息安全需求。云服务商确保其下级供应商采取了必要的安全措施。云服务商还应为客户提供与安全措施有关的文档和信息，配合客户完成对信息系统和业务的管理
安全要求 2：系统与通信保护	云服务商应在云计算平台的外部边界和内部关键边界上监视、控制和保护网络通信，并采用结构化设计、软件开发技术和软件工程方法有效保护云计算平台的安全性
安全要求 3：访问控制	云服务商应严格保护云计算平台的客户数据和用户隐私，在授权信息系统用户及其进程、设备（包括其他信息系统的设备）访问云计算平台之前，应对其进行身份标识及鉴别，并限制授权用户可执行的操作和使用的功能
安全要求 4：配置管理	云服务商应对云计算平台进行配置管理，在系统生命周期内建立和维护云计算平台（包括硬件、软件、文档等）的基线配置和详细清单，并设置和实现云计算平台中各类产品的安全配置参数



续表

云服务安全要求	安全控制目标
安全要求 5：维护	云服务商应定期维护云计算平台设施和软件系统，并对维护所使用的工具、技术、机制以及维护人员进行有效控制，且做好相关记录
安全要求 6：应急响应与灾备	云服务商应为云计算平台编制应急响应计划，并定期演练，确保在紧急情况下重要信息资源的可用性。云服务商应建立事件处理计划，包括对事件的预防、检测、分析、控制、恢复及用户响应活动等，对事件进行跟踪、记录并向相关人员报告。服务商应具备灾难恢复能力，建立必要的备份设施，确保客户业务可持续
安全要求 7：审计	云服务商应根据安全需求和客户要求，制定可审计事件清单，明确审计记录内容，实施审计并妥善保存审计记录，对审计记录进行定期分析和审查，还应防范对审计记录的未授权访问、篡改和删除行为
安全要求 8：风险评估与持续监控	云服务商应定期或在威胁环境发生变化时，对云计算平台进行风险评估，确保云计算平台的安全风险处于可接受水平。服务商应制定监控目标清单，对目标进行持续安全监控，并在异常和非授权情况发生时发出警报
安全要求 9：安全组织与人员	云服务商应确保能够接触客户信息或业务的各类人员（包括供应商人员）上岗时具备履行其信息安全责任的素质和能力，在授予相关人员访问权限之前对其进行审查并定期复查，在人员调动或离职时履行安全程序，对于违反信息安全规定的人员进行处罚
安全要求 10：物理与环境保护	云服务商应确保机房位于中国境内，机房选址、设计、供电、消防、温湿度控制等符合相关标准的要求。云服务商应对机房进行监控，严格限制各类人员与运行中的云计算平台设备进行物理接触，确需接触的，需通过云服务商的明确授权

# 数据本地化与跨境传输

目前，我国已经发展成世界第二大经济体，世界第一贸易大国，这意味着在数字化时代，在大型跨国互联网企业快速发展的背景下，货物、人员、服务的流动交织着数据的流动，我国也将逐渐成为最大的数据贸易国。加之云计算、大数据等新一代信息技术与跨境电子商务的蓬勃发展，促使数据跨境流动成为常态，数据本身所承载的经济价值日益凸显。而“棱镜门”事件的爆发，以及近年来大规模的数据泄露事件频频发生，其中针对关键信息基础设施的数据泄露更是会威胁国家安全和社会稳定，使得数据的安全性也逐渐引起各国高度关注。

如何平衡数据所蕴涵的安全与发展之间的关系已经成为摆在各国面前的现实问题，数据本地化的立法政策作为一种规制数据跨境较为有效的措施，使得各国掀起了围绕“数据本地化”的立法浪潮，包括俄罗斯、巴西、澳大利亚、欧盟等国家和地区都纷纷出台立法或制定政策，规范本国数据的境外传输，我国也于2016年11月7日正式公布了《网络安全法》，其中第三十七条对关键信息基础设施运营者在境内收集和产生的个人信息和重要数据的存储和传输做出了本地化的要求。

## 第一节 《网络安全法》相关规定及释义

《网络安全法》第三十七条规定了数据本地化制度，即关键信息基础设施的运

营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定。

《网络安全法》是我国首次在网络安全领域基本法层面规定数据本地化制度，充分说明在信息化时代，数据安全对于国家、社会和公民的重要性以及在激烈的国际竞争中数据的价值。首先，就第三十七条而言，可以看出国家将保护的对象放在个人信息和重要数据上，并不针对全部网络运营者的所有数据，做到了有重点地进行保护。其次，基本的要求是在境内存储，在某些情况下确需向境外提供时，应通过安全评估加以限制。国家通过两个阶段的规定试图寻求安全与发展之间的平衡。相较于《网络安全法（草案）》<sup>①</sup>和二次审议稿<sup>②</sup>的相关规定，基本思路保持一致，对于在中国境内收集和产生的特定数据应在境内存储，如确需出境的，由国家网信部门会同有关部门进行评估。但经过最终审议，首先，该规定将境内存储的对象扩展为“在中华人民共和国境内运营中收集和产生的个人信息和重要数据”，将个人信息和重要数据进行等同规定，并删除“业务”二字。其次，将数据跨境的目的规定为“提供”，删除了草案中的“在境外存储”模式。

但第三十七条的规定过于宽泛，对于主体、个人信息和重要数据的识别、向境外提供等概念没有给出明确规定，需要相关后续配套制度加以界定，以增加可操作性。

## 第二节 数据本地化

### 一、数据本地化制度概述

数据本地化并不完全以强制要求数据的本地化存储进行实现，除特定数据（如

---

① 2015 年 6 月，第十二届全国人大常委会第十五次会议初次审议了《网络安全法（草案）》。其中，第三十一条规定：关键信息基础设施的运营者应当在中华人民共和国境内存储在运营中收集和产生的公民个人信息等重要数据；因业务需要，确需在境外存储或者向境外的组织或者个人提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估。法律、行政法规另有规定的从其规定。

② 2016 年 6 月，第十二届全国人大常委会第二十一次会议对草案二次审议稿进行了审议。其中，第三十五条规定：关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的公民个人信息和重要业务数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定。

国家公共数据)外,强制性的数据本地化存储存在滥用贸易壁垒之嫌。因此,在更为广泛的情况下,通过设置数据跨境限制来实现数据本地化是更为有效的方法。基于上述的利益考量以及各国数据保障能力的不同,现在主要的本地化政策包括两种模式。

### (一) 禁止数据出境

禁止数据出境此种模式采取绝对化的禁止数据出境,在互联互通的当代环境下适用范围较为狭窄,通常仅针对涉及国家安全或公共信息的特定数据。该模式严苛地保护了涉及国家核心或敏感数据的安全,在国际竞争激烈的背景下有一定存在的必要性,但缺点在于对执法过程中数据客体的认定以及一致性的保持要求较高。

在国际社会法律实践中,印度《公共记录法》第四章规定:禁止公共记录传输到印度境外,但基于公共目的传输除外。同时,该法规定:“任何由计算机生成的材料”都属于“公共记录”。澳大利亚《个人电子健康记录控制法案》第七十七条规定:禁止将记录转移至澳大利亚境外。在我国保守国家秘密、征信业、金融、人口健康等领域中也有禁止相关数据出境的规定。

### (二) 要求数据中心建在境内

数据中心作为重要的网络基础设施,用于提供系统、数据的集成、存储、处理、分析等的场所及相关服务。此种模式下要求将数据中心设置建在境内,可以使数据的整个生命周期均位于境内,提高对数据的控制力。但由于建设数据中心成本较高,一定程度上容易降低对外企的吸引力。同时,为避免数据集中产生的“蜜罐”效应,也需要国内网络环境有足够的保障能力和技术发展水平。

在国际范围内此类立法实践体现为法国要求电子通信拦截系统建立在境内,印度尼西亚要求公共服务电子系统运营者的数据中心和容灾备份中心设置在境内。而我国在《国务院关于大力推进信息化发展和切实保障信息安全的若干意见》中“第六条规定,为政府机关提供服务的数据中心、云计算服务平台等要设在境内。”类似地要求包括存放地图数据的服务器、从事网络出版服务的出版单位所需的必要服务器和存储设备,以及网约车的个人信息和生成的业务数据都要求将其数据中心建在境内。对于近年来兴起的互联网租赁自行车,即共享单车的规范与管理,交通运输

部等十部门 2017 年 8 月 1 日公布的《关于鼓励和规范互联网租赁自行车发展的指导意见》中也要求将服务器设在中国大陆境内，在境内运营中采集的信息和生成的相关数据应当在中国大陆境内存储。国外主要国家数据本地化立法汇总如表 16-1 所示。

表 16-1 国外主要国家数据本地化立法汇总

禁止数据 离境	澳大利亚	不得将记录携带至澳大利亚境外，不允许在澳大利亚境外持有记录； 不得在澳大利亚境外处理关于记录的各种信息
	印度	禁止公共记录传输到印度境外，但基于公共目的的传输除外
数据中心 建在境内	法国	要求服务提供商提供的电子通信拦截系统要在法国境内建立和实施
	印度尼西亚	公共服务电子系统运营者将数据中心和容灾备份中心设置在境内
	俄罗斯	商业机构有义务确保俄公民个人数据的处理活动均应使用俄联邦境内的服务器

## 二、数据本地化的法规遵从框架及建议

我国在颁布《网络安全法》之前，对于数据跨境流动的规制散见于其他法律法规中，模式主要包括禁止数据离境、将数据中心建在境内两种。《网络安全法》公布之后，规定由国家网信部门统筹，其余主管部门在各自职责范围内配合的管理体制，将数据跨境流动制度在基本法层面加以规定，并通过进一步制定实施细则加以落实，实现了我国数据跨境流动的法治化进程。

### （一）禁止数据离境的法规遵从框架及建议

严苛的禁止数据离境模式仅限于涉及国家安全、社会稳定和个人利益的个别领域。在当前互联网与各行业深度融合的驱动下，以电子数据为表现形式的存储更为普遍，因此，在近年来的国家立法中对于禁止数据离境的规定也有所增加。数据本地化中禁止数据离境制度的法规遵从框架如表 16-2 所示。

表 16-2 数据本地化中禁止数据离境制度的法规遵从框架

法律名称	法律条款	法律规定
《保守国家秘密法》	第四十八条	违反本法规定，邮寄、托运国家秘密载体出境，或者未经有关主管部门批准，携带、传递国家秘密载体出境的，依法给予处分，构成犯罪的，依法追究刑事责任
《中国人民银行关于银行业金融机构做好个人金融信息保护工作的通知》	第六条	在中国境内收集的个人金融信息的储存、处理和分析应当在中国境内进行。除法律法规及中国人民银行另有规定外，银行业金融机构不得向境外提供境内个人金融信息

续表

法律名称	法律条款	法律规定
《征信业管理条例》	第二十四条	征信机构在中国境内采集的信息的整理、保存和加工，应当在中国境内进行
《人口健康信息管理办法（试行）》	第十条	不得将人口健康信息在境外的服务器中存储，不得托管、租赁在境外的服务器
《网络借贷信息中介机构业务活动管理暂行办法》	第二十七条	在中国境内收集的出借人与借款人信息的储存、处理和分析应当在中国境内进行。除法律法规另有规定外，网络借贷信息中介机构不得向境外提供境内出借人和借款人信息

鉴于我国目前对于禁止数据离境没有进一步的细则加以明确，当网络运营商涉及上述敏感领域或行业时，应遵循相应法律规定，禁止数据离境。

（二）数据中心建在境内的法规遵从框架及建议

将数据中心建在境内在一定程度上将提升我国对于保护的个人信息和重要数据的管控力度，提升国家保障能力。因此，在涉及国家安全的关键领域以及收集大量公民个人信息的行业内，我国正逐渐建立完善的数据中心建在境内的法律要求。数据本地化中数据中心建在境内制度的法规遵从框架如表 16-3 所示。

表 16-3 数据本地化中数据中心建在境内制度的法规遵从框架

法律名称	法律条款	法律规定
《国务院关于大力推进信息化发展和切实保障信息安全的若干意见》	六（二）	为政府机关提供服务的数据中心、云计算服务平台等要设在境内
《信息安全技术云计算服务安全能力要求》	14.2.1	云服务商应确保云计算服务器及运行关键业务和数据的物理设备位于中国境内
《地图管理条例》（国务院第 664 号）	第三十四条	互联网地图服务单位应当将存放地图数据的服务器设在中华人民共和国境内
《网络出版服务管理规定》（国家新闻出版广电总局令第 5 号）	第八条	图书、音像、电子、报纸、期刊出版单位从事网络出版服务，应当具备以下条件：……（三）有从事网络出版服务所需的必要的技术设备，相关服务器和存储设备必须存放在中华人民共和国境内
《网络预约出租汽车经营服务管理暂行办法》	第二十七条	网约车平台公司所采集的个人信息和生成的业务数据，应当在中国内地存储和使用，保存期限不少于 2 年，除法律法规另有规定外，上述信息和数据不得外流

续表

法律名称	法律条款	法律规定
《网络安全法》	第三十七条	关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定
《关于鼓励和规范互联网租赁自行车发展的指导意见》	(十三)	加强网络和信息安全保护。……将服务器设在中国大陆境内……在境内运营中采集的信息和生成的相关数据应当在中国大陆境内存储

根据《网络安全法》第三十七条前半段的规定，我国关键信息基础设施运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。将海量数据存储在国内，为避免“蜜罐”效应，需要从技术和制度两方面来保障数据的安全。全国信息安全标准化技术委员会 2011 年公布的《计算机场地通用规范》和 2017 年 8 月 25 日公布《信息安全技术 网络存储安全技术要求》（征求意见稿），分别对计算机场地建设要求和网络存储安全做出要求，也为网络运营者的遵从提供了指引。数据本地化制度中将数据中心建在境内制度的法规遵从建议如表 16-4 所示。

表 16-4 数据本地化制度中将数据中心建在境内制度的法规遵从建议

控制项	数据中心建在境内制度的法规遵从建议	对应条款
1. 网络存储安全功能要求		第三十七条
访问安全	组织应通过保证所有开放的端口都是系统运行和维护所必需的，通信端口支持可被关闭等措施保证介入访问方式安全。 组织应按访问控制安全策略进行设计，实现对策略控制下的存储数据的访问控制功能。 组织应通过在网络存储自身和远程访问端之间、本地访问之间提供一条通信路径，此路径在逻辑上与其他通信路径截然不同，并且能够对其节点提供确定的标识，以及保护通信数据免遭修改或泄露等措施保障的可信路径安全	关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定。
系统安全	组织应保证自身安全可靠运行，支持自动查看设备的工作状态，当监测数值超过预先设定的故障阈值时，提供报警功能；提供系统完整性保护功能；若网络存储自带操作系统、数据库、Web 应用，应保证系统软件及软件运行环境不存在高风险级别的漏洞，例如通用漏洞评分系统（Common Vulnerability Scoring System, CVSS）评分 7 分及以上的漏洞。 组织应支持对操作系统、数据库、文件系统进行安全加固，提供 Web 安全功能，支持在设备启动时对软件和固件进行完整性验证，以及在固件升级和安装过程中对固件进行完整性校验	

续表

控制项	数据中心建在境内制度的法规遵从建议	对应条款
数据安全	<p>组织应通过支持数据安全擦除，数据擦除后不可恢复等措施首先保证存储介质安全，其次对网络存储产品中存储的数据进行完整性和保密性保护。在对资源进行动态管理的存储中，提供剩余信息保护功能。</p> <p>组织应提供对数据进行备份和恢复的能力，支持第三方防病毒软件扫描和通过配置独立磁盘冗余阵列（Redundant Array of Independent Disks, RAID）保障存储数据的可靠性。</p> <p>组织应支持双活功能，当一个数据中心的存储系统发生故障时，业务自动切换到另一个数据中心</p>	
管理安全	<p>组织应为每个用户提供唯一的身份标识，对每个用户身份标识进行管理、维护，确保其不被非授权地访问、修改或删除；将用户身份标识和该用户的所有可审计事件相关联。</p> <p>组织应提供账号管理功能，保证系统中的账号具有唯一性，应禁止预留任何的未公开账号，所有账号都必须可被系统管理，并在资料中提供所有账号及管理操作说明等措施。</p> <p>组织应提供对用户的鉴别功能、登录认证功能和会话管理功能，并且至少提供基于口令的鉴别方式。</p> <p>组织应进行安全审计，妥善存储和管理审计数据。组织应为自身的运行提供时间标记，即应有时钟系统（如计时时钟、中断时钟等），并提供时间戳服务，提供数字证书管理功能。</p> <p>组织应支持第三方密钥管理产品对存储进行必要的密钥管理支撑；提供隐私保护声明，至少表明网络存储不感知用户业务数据</p>	
2. 网络存储安全保障要求		
开发	<p>组织应提供产品安全功能的安全架构描述、功能规范和产品设计文档。</p> <p>组织应按详细级别定义产品安全功能，详细级别应达到无须进一步设计就能生成安全功能的程度，以开发人员使用的形式提供；提供产品设计描述与实现表示实例之间的映射，并证明其一致性</p>	
指导性文档	<p>组织应提供明确和合理的操作用户指南，操作用户指南与为评估而提供的其他所有文档保持一致，对每种用户角色的描述应满足一定要求。</p> <p>组织应提供产品及其准备程序，准备程序描述应满足以下要求： 描述与开发者交付程序相一致的安全接收所交付产品必需的所有步骤； 描述安全安装产品及其运行环境必需的所有步骤</p>	
生命周期支持	<p>组织应使用配置管理系统，并提供配置管理文档和产品配置项列表。</p> <p>组织应使用一定的交付程序交付产品，并将交付过程文档化。在给用户方交付产品的版本时，交付文档应描述为维护安全所必需的所有程序，以及产品交付安装包的防病毒扫描结果和产品解决的安全漏洞列表</p>	



续表

控制项	数据中心建在境内制度的法规遵从建议	对应条款
测试	<p>组织应提供测试深度的分析，测试产品安全功能，将结果文档化并提供测试文档。</p> <p>组织应提供一组与其自测安全功能时使用的同等资源，以用于安全功能的抽样测试，该测试由产品开发团队之外的测评机构或测评团队完成。</p> <p>组织应对产品代码进行静态安全扫描，并解决高风险的问题，提供相应的分析报告。若产品涉及开源或第三方软件，组织应提供开源及第三方软件使用列表、开源及第三方软件选型与安全评估分析</p>	
脆弱性评定	<p>基于已标识的潜在脆弱性，组织应保证产品能够抵抗以下攻击行为：</p> <p>具有基本攻击潜力的攻击者的攻击；</p> <p>具有增强型基本攻击潜力的攻击者的攻击</p>	
3. 计算机场地建设要求		
技术要求	<p>组织应依据计算机系统的规模、用途以及管理体制，选用下列房间。</p> <p>主要工作房间：计算机机房、终端室等。</p> <p>第一类辅助房间：低压配电间、不间断电源室、蓄电池室、空调机室、发电机室、气体钢瓶室、监控室等。</p> <p>第二类辅助房间：资料室、维修室、技术人员办公室。</p> <p>第三类辅助房间：储藏室、缓冲间、技术人员休息室、盥洗室等。</p> <p>组织应根据要求确定计算机机房面积和净高，安装符合要求的活动地板、建筑结构、环境条件、供电系统等</p>	
安全防护	<p>组织应建立完善的计算机场地防雷和防水措施、配置健全的消防系统、入侵报警系统、视频监控系统、出入口控制系统和电磁屏蔽室</p>	
测试方法	<p>组织应采用目测法检验，按规模、用途等确定的房间数符合技术要求。</p> <p>组织应进行温度测试、湿度测试、尘埃测试、照度测试、噪声测试、电磁场干扰环境场强测试、电压和频率测试、波形畸变率测试、接地电阻测试、屏蔽室效能测试、综合布线测试、火灾自动报警系统测试、气体灭火系统测试、入侵报警系统测试、视频监控系统测试、出入口控制系统测试</p>	
验收规则	<p>计算机场地在用户接收前应进行验收。验收应由建设单位负责组织实施、施工和监理等部门共同进行，或由国家认可的质量检验单位负责进行。</p> <p>验收后应提交验收报告，验收过程有某项通不过验收时应查明原因，返修后重新进行该项目的验收，若再通不过验收时，则判未通过验收。</p> <p>计算机场地验收未通过，不准投入使用</p>	

### 第三节 数据跨境传输安全评估

#### 一、数据跨境传输安全评估的制度概述

数据跨境前进行安全评估，相当于对数据进行“体检”，将可能危及国家安全、社会公共利益或个人合法权益的数据不予出境，赋予国家主动权，也有助于形成社会认同感和信任感。但鉴于安全评估程序及内容较为烦琐，实施细则制定过于精细或过于模糊都不利于实践的执行，因此，需要合理谨慎地确定评估对象、主体、内容及方式。

该模式可以较好地实现安全与发展之间的平衡，因此此种模式是接受国家较多并且形式较为丰富的一种，具体还可分为确保数据接收国有同等的安全保护水平，以及数据主体同意或部长特别指定地区进行传输两种模式。首先，确保数据接收国有同等的安全保护水平。欧盟 2018 年生效的《通用数据保护条例》中规定由委员会对数据接收国的法治水平、监督管理能力和承担的国际义务等内容进行评估，从而确保同等的数据安全保护水平。其次，经数据主体同意或部长特别指定地区进行传输，我国的《网络安全法》和 2013 年的《信息安全技术公共及商用服务信息系统个人信息保护指南》中体现了相应规定。国外主要国家数据跨境传输安全评估制度的立法汇总如表 16-5 所示。

表 16-5 国外主要国家数据跨境传输安全评估制度的立法汇总

数据传输 安全评估	欧盟	在数据传输前由委员会对数据接收国进行安全评估，并定期审查
	新加坡	确保组织能够对传输的个人数据提供与本国法规定的同等标准的保护
	日本	个人信息可以传输到日本委员会认可的、与日本国内保护水平相当的国家或地区
	巴西	跨境数据传输时，数据接收国的个人数据保护必须达到充分性保护的 水平
	印度	确保同等的数据保护水平
	马来西亚	数据使用者不能将个人数据传输到境外，但部长特别指定的地方除外
	韩国	数据离境要通知并获得信息主体的同意，并提供数据输送的详细信息

二、数据跨境传输安全评估的法规遵从框架及建议

《网络安全法》第三十七条后半段对我国数据出境前安全评估制度做出规定，填补了我国在法律层面上该项制度的空白。目前我国仅在《信息安全技术公共及商用服务信息系统个人信息保护指南》和《网络安全法》中体现了该项制度。数据跨境安全评估的法规遵从框架如表 16-6 所示。

表 16-6 数据跨境安全评估的法规遵从框架

法律名称	法律条款	法律规定
《信息安全技术公共及商用服务信息系统个人信息保护指南》	第 5.4.5 条	未经个人信息主体的明示同意，或法律法规明确规定，或未经主管部门同意，个人信息管理者不得将个人信息转移给境外个人信息获得者，包括位于境外的个人或境外注册的组织和机构
《网络安全法》	第三十七条	关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定

为贯彻落实《网络安全法》第三十七条中关于数据出境前安全评估制度的规定，2017 年 4 月 11 日，国家网信部门制定公布了《个人信息和重要数据出境安全评估办法（征求意见稿）》（以下简称《办法》），共十八条，对出境安全评估的主体、对象、范围、方式、保障措施等内容加以规定，内容虽在可操作性层面有所欠缺，但涉及范围较为全面。

为解决《办法》的可操作性问题，2017 年 8 月 30 日，全国信息安全标准化技术委员会公布了国家标准《信息安全技术 数据出境安全评估指南（征求意见稿）》（以下简称《指南》）。在《指南》中进一步对个人信息和重要数据的界定及范围加以明确，对安全评估的具体程序及评估内容加以规定。

从整体来说，《办法》和《指南》是在坚持保障个人信息和重要数据安全的价值引导下，积极寻求数据安全与自由流动之间的利益平衡，通过规定评估对象、评估主体、评估内容、评估方式、保障措施等内容为数据跨境保驾护航。

（一）评估对象

作为一项具体应用的制度，首先应确定评估对象，从而围绕该评估对象所涉

及各利益相关方确定评估主体，根据评估对象自身重要等级或行业特性来明晰评估内容及方式。评估对象的范围大小、严苛程度将在一定程度上反映国家对于所涉及法益的保护力度。就数据出境前安全评估这项制度而言，其评估对象从《网络安全法》到《办法》有扩大的趋势。《网络安全法》第三十七条规定：关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估。而《办法》第二条则规定了“网络运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储，因业务需要，确需向境外提供的，应当按照本《办法》进行安全评估”。从规制关键信息基础设施运营者拓展到对所有网络运营者的共同要求，这样的变化充分体现了跨境数据对于国家安全、社会稳定和个人权益保护的重要影响，以及国家对其安全状况的审慎态度。

《办法》第二条对于评估对象范围扩大的法律依据可从第一条<sup>①</sup>中获得。在第一条中指出，《办法》的制定依据为《国家安全法》和《网络安全法》等法律法规。《网络安全法》涉及的法条为第三十七条，而《国家安全法》中体现为第二十五条：“国家建设网络与信息安全保障体系，提升网络与信息安全保护能力，加强网络和信息技术的创新研究和开发应用，实现网络和信息核心技术、关键基础设施和重要领域信息系统及数据的安全可控；加强网络管理，防范、制止和依法惩治网络攻击、网络入侵、网络窃密、散布违法有害信息等网络违法犯罪行为，维护国家网络空间主权、安全和发展利益”。结合两者的要求，我国进行跨境数据流动法律规制的目的在于保障数据依法有序自由流动，保障个人信息和重要数据的安全。而就当前实际情况而言，不仅仅是关键信息基础设施运营者需要管理，其他网络运营者也掌握着大量数据，能够对公民的个人隐私和国家安全造成一定影响。如果不对其进行管理，任由其自由跨境流动，则难以真正维护数据的安全可控，实现该项制度建立的题中应有之义。

在《指南》中，通过 3.2 境内运营和 3.7 数据出境的具体限定和排除性规定，

---

① 《个人信息和重要数据出境安全评估办法（征求意见稿）》第一条 为保障个人信息和重要数据安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，根据《国家安全法》、《网络安全法》等法律法规，制定本办法。

网络运营者可先判定自身是否属于评估对象范围，从而决定是否进行后续程序。

除此之外，《办法》第十六条对其他评估对象进行了补充性规定，要求其他个人和组织在中华人民共和国境内运营中收集和产生的个人信息和重要数据出境的安全评估工作参照本办法执行，这使得管理体系更加完整严密。

由此可以看出，国家在制定落实安全评估制度时对相关法益保护程度的反复考量与权衡，也从侧面印证了“没有网络安全，就没有国家安全”这一基本理念。

## （二）评估主体

根据《办法》的相关规定，我国数据跨境前安全评估的主体包括网络运营者、行业主管或监管部门、国家网信部门。

网络运营者的义务来源体现为：《网络安全法》第九条规定，网络运营者开展经营活动和服务活动，必须遵守法律、行政法规，尊重社会公德，遵守商业道德，诚实信用，履行网络安全保护义务，接受政府和社会的监督，承担社会责任，以及《网络安全法》第四十二条规定，网络运营者应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、损毁流失。

在实施细节方面，《办法》第七条明确规定：网络运营者应在数据出境前，自行组织对数据出境进行安全评估，并对评估结果负责。第十二条也提到网络运营者应根据业务发展和网络运营情况，每年对数据出境至少进行一次安全评估。当数据接收方出现变更，数据出境目的、范围、数量、类型等发生较大变化，数据接收方或出境运营发生重大安全事件时，应及时重新进行安全评估。

安全评估制度的另一主体是具体的行业主管部门或监管部门及国家网信部门。《网络安全法》第三十二条规定：按照国务院规定的职责分工，负责关键信息基础设施安全保护工作的部门分别编制并组织实施本行业、本领域的关键信息基础设施安全规划，指导和监督关键信息基础设施运行安全保护工作。关键信息基础设施保护部门即行业主管监管部门，其对跨境数据的安全性也应该承担监督管理责任。

出于行政资源优化配置的考虑，行业主管部门仅在法律规定的特别情况下对

拟跨境数据的安全性进行评估。《办法》第九条<sup>①</sup>做出了细化性的规定，列举了若干情形，并通过第六项（其他可能影响国家安全和社会公共利益，行业主管或监管部门认为应该评估。行业主管或监管部门不明确的，由国家网信部门组织评估）做出兜底性规定。与此同时，鉴于当前大型互联网企业或跨国企业业务范围广泛，跨境数据行业涉及情况也较为复杂，不可避免将出现行业主管和监管部门不明确的情况，对此《办法》规定，出现上述情况时，由国家网信部门来组织评估。

由此可以看出，一方面，国家在考量评估主体及其职责分工时的审慎态度，通过规定全面的各层级的评估主体，避免出现实践层面的空白，提升法律法规的有效性和权威性，防止不法网络运营者钻法律的空子。另一方面，对于评估内容的谨慎分类，使得行业主管或监管部门可以更好地维护涉及国家安全和社会稳定的数据的安全，实现立法目的。

### （三）评估内容及方式

跨境数据安全评估是一项同时涉及境内外数据安全的制度，因此评估内容应涉及数据出境前其本身的安全性、相关数据主体权利保护情况，以及出境后可能面临风险的保障能力。我国目前的安全评估内容主要体现为《办法》第八条。首先是评估数据出境的必要性，其次是针对个人信息和重要数据本身安全情况的确定，最后是数据接收方及其所在国家和地区的安全保护水平，以及数据出境后可能面临的风险评估。对于评估内容，《指南》中进行了更为详尽的规定，其通过等级判定与赋值的方式，将个人信息、重要数据出境风险可控程度的评估流程分别加以明确。

在上述几项内容的评估过程中有可能出现以下两种情况。第一，当拟出境的个人信息或重要数据体量较大，或者涉及国家核心及敏感数据等情况时需交由行业主管或监管部门进行评估，即《办法》第九条之规定。第二，当个人信息出境未经个人信息主体同意，或可能侵害个人利益，或数据出境给国家政治、经济、

① 《个人信息和重要数据出境安全评估办法（征求意见稿）》第九条 出境数据存在以下情况之一的，网络运营者应报请行业主管或监管部门组织安全评估：（一）含有或累计含有 50 万人以上的个人信息；（二）数据量超过 1 000GB；（三）包含核设施、化学生物、国防军工、人口健康等领域数据，大型工程活动、海洋环境，以及敏感地理信息数据等；（四）包含关键信息基础设施的系统漏洞、安全防护等网络安全信息；（五）关键信息基础设施运营者向境外提供个人信息和重要数据；（六）其他可能影响国家安全和社会公共利益，行业主管或监管部门认为应该评估。行业主管或监管部门不明确的，由国家网信部门组织评估。

科技、国防等安全带来风险，可能出现影响国家安全、损害社会公共利益等情况时，该数据不得出境，即《办法》第十一条之规定。

再评估义务规定为《办法》第十二条，即“当数据接收方出现变更，数据出境目的、范围、数量、类型等发生较大变化，数据接收方或出境数据发生重大安全事件时，应及时重新进行安全评估”。这就使得安全评估制度更具活力，不仅仅是出具一份评估报告就算义务履行完毕，而是真正以维护国家网络主权与秩序、促进数据有序流动为目的进行适时的评估与管理。

就评估方式而言，主要体现为《办法》第七条规定的网络运营者自评估的方式。在《指南》3.9 中更是进一步明确网络运营者依照相关国家法律法规和标准的规定，自行组织或委托网络安全服务机构对数据出境开展安全评估。4.2.3 要求网络运营者组建数据出境安全自评估工作组，工作组主要包含法务、政策、安全、技术、管理相关专业人员。数据出境安全自评估工作组应负责审查业务部门提交的数据出境计划，并定期对数据出境情况开展检查、抽查。

由企业自行评估需要注意以下两点内容。第一，由企业自行评估赋予企业一定主动权，在不涉及《办法》第九条规定的情形时，如何评价企业评估能力，保证落实相关评估标准的一致性，以及如何养成信息主体对于评估结果的信任，需要行业主管或监管部门与企业一起构建安全评估制度的社会信任体系。第二，赋予自评估的义务将不可避免地增加企业运营成本，在当前市场竞争激烈，各大企业竞相拓展业务版图的环境下，需提高企业安全意识，在落实安全评估制度过程中正确处理安全与发展之间的平衡。数据跨境安全评估的法规遵从建议如表 16-7 所示。

表 16-7 数据跨境安全评估的法规遵从建议

控制项	数据出境前安全评估制度的法规遵从建议	对应条款
1. 评估对象		第三十七条
境内运营的要求	组织应在中华人民共和国境内开展业务，提供产品或服务的活动。 未在中华人民共和国境内注册的网络运营者，但在中华人民共和国境内开展业务，或向中华人民共和国境内提供产品或服务的，属于境内运营。判断网络运营者是否在中华人民共和国境内开展业务，或向中华人民共和国境内提供产品或服务的参考因素包括但不限于：使用中文；以人民币作为结算货币；向中国境内配送物流等。 中华人民共和国境内的网络运营者仅向境外机构、组织或个人开展业务、提供商品或服务，且不涉及境内公民个人信息和重要数据的，不视为境内运营	关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定

续表

控制项	数据出境前安全评估制度的法规遵从建议	对应条款
拟出境数据的要求	<p>组织拟出境的个人信息应是以电子或其他方式记录的能够单独或与其他信息结合识别自然人身份的各种信息,如姓名、出生日期、身份证号、个人账号信息、住址、电话号码、指纹、虹膜等。</p> <p>组织拟出境的重要数据应是相关组织、机构和个人在境内收集、产生的不涉及国家秘密,但与国家安全、经济发展,以及公共利益密切相关的数据(包括原始数据和衍生数据)。经政府信息公开渠道合法公开的,不再属于重要数据</p>	
数据出境的要求	<p>组织的数据出境是指通过网络等方式,将其在中华人民共和国境内运营中收集和产生的个人信息和重要数据,通过直接提供或开展业务、提供服务、产品等方式提供给境外的机构、组织或个人的一次性活动或连续性活动。</p> <p>以下情形属于数据出境:</p> <p>向本国境内,但不属于本国司法管辖或未在境内注册的主体提供个人信息和重要数据;</p> <p>数据未转移存储至本国以外的地方,但被境外的机构、组织、个人访问查看的(公开信息、网页访问除外);</p> <p>网络运营者集团内部数据由境内转移至境外,涉及其在境内运营中收集和产生的个人信息和重要数据的。</p> <p>非在境内运营中收集和产生的个人信息和重要数据经由本国出境,未经任何变动或加工处理的,不属于数据出境。</p> <p>非在境内运营中收集和产生的个人信息和重要数据在境内存储、加工处理后出境,不涉及境内运营中收集和产生的个人信息和重要数据的,不属于数据出境</p>	
2. 评估主体		
自行评估的要求	<p>组织应建立数据出境安全自评估工作组,工作组主要包含法务、政策、安全、技术、管理相关专业人员。数据出境安全自评估工作组应负责审查业务部门提交的数据出境计划,并定期对数据出境情况开展检查、抽查。</p> <p>组织应在满足以下条件之一时启动评估:</p> <p>涉及数据出境的;</p> <p>关键信息基础设施运营者进行数据出境之前的;</p> <p>已完成数据出境安全自评估的产品或业务所涉及的个人信息和重要数据出境,在目的、范围、类型、数量等方面发生较大变化、数据接收方变更或发生重大安全事件的;</p> <p>按照行业主管或者监管部门要求启动的。</p>	



续表

控制项	数据出境前安全评估制度的法规遵从建议	对应条款
自行评估的要求	<p>网络运营者在完成数据出境安全自评估后，应形成安全自评估报告。安全自评估报告内容应包括但不限于：安全自评估对象基本情况、安全自评估组织实施情况、安全自评估结果、数据出境安全风险点、检查修正建议。安全自评估报告应至少保存 2 年，并在如下情况下将安全自评估报告上报行业主管部门，行业主管部门不明确的，报国家网信部门。</p> <p>关键信息基础设施运营者开展的安全自评估：</p> <p>一年内出境的个人信息数量达到国家网信部门、行业主管部门上报要求的；</p> <p>包含核设施、生物化学、国防军工、人口健康等领域数据，大型工程活动、海洋环境敏感地理信息数据，以及其他重要数据的；</p> <p>涉及关键信息基础设施的安全缺陷、具体安全防护措施等网络安全信息的；</p> <p>其他可能影响国家安全、经济发展和社会公共利益的。</p> <p>如果安全自评估结果为禁止出境的，组织应采用相关措施降低数据出境安全风险，并修正数据出境计划，重新开展安全自评估</p>	
主管部门评估的要求	<p>国家网信部门、行业主管部门根据数据出境类型、数量、范围、重要程度等，酌情组织开展主管部门评估。具有下列情形之一的，国家网信部门、行业主管部门可启动主管部门评估：</p> <p>一年内出境的个人信息数量达到国家网信部门、行业主管部门上报要求的；</p> <p>包含核设施、生物化学、国防军工、人口健康等领域数据，大型工程活动、海洋环境、敏感地理信息数据，以及其他重要数据的；</p> <p>涉及关键信息基础设施的安全缺陷、具体安全防护措施等网络安全信息的；</p> <p>关键基础设施运营者数据出境的；</p> <p>其他可能影响国家安全、经济发展和社会公共利益的；</p> <p>大量用户投诉、举报的；</p> <p>全国性行业协会建议的；</p> <p>其他经国家网信部门、行业主管部门认定有必要启动主管部门评估的</p>	
3. 评估内容		
	<p>组织在评估出境目的时，应同时满足合法性、正当性和必要性的要求。</p> <p>合法性包括以下情况：</p>	

续表

控制项	数据出境前安全评估制度的法规遵从建议	对应条款
出境目的的 评估要求	<p>不属于法律法规明令禁止的。</p> <p>不属于国家网信部门、公安部门、安全部门等有关部门认定不能出境的。</p> <p>拨打国际及漫游电话、发送国际电子邮件、进行国际即时通信、通过互联网进行跨境交易以及其他个人主动行为，视为个人信息主体已经同意。</p> <p>将合法向社会公开披露的个人信息出境，视为个人信息主体已经同意。</p> <p>网络运营者在取得个人信息主体同意前，应将数据出境目的、类型、数据接收方情况及数据出境可能存在的风险，网络运营者的联系人及其联系方式等信息明确告知个人信息主体。</p> <p>当网络运营者隐私规则发生变更、数据出境目的、范围、类型、数量发生较大变化、数据接收方发生变更或数据出境风险发生较大变化时应重新取得个人信息主体同意。</p> <p>正当性包括以下情况：</p> <p>个人信息主体已同意的，虽未经个人信息主体同意但是危及公民生命财产安全等紧急情况除外；</p> <p>不违反相关主管部门规定的。</p> <p>必要性包括以下任一种或几种情况：</p> <p>履行合同义务所必需的；</p> <p>同一机构、组织内部开展业务所必需的；</p> <p>我国政府部门履行公务所必需的；</p> <p>履行我国政府与其他国家和地区、国际组织签署的条约、协议所必需的；</p> <p>其他维护网络空间主权和国家安全、经济发展、社会公共利益和保护公民合法权益需要的</p>	
安全风险的 评估要求	<p>组织应综合考虑出境数据的属性和数据出境发生安全事件的可能性及影响程度。</p> <p>数据属性：</p> <p>个人信息的属性，包括类型、数量、范围、敏感程度和技术处理情况等；</p> <p>重要数据的属性，包括类型、数量、范围和技术处理情况等；</p> <p>当数据出境同时包含个人信息和重要数据时，应同时满足上述两条评估要求。</p> <p>数据出境发生安全事件的可能性及影响程度：</p> <p>发送方数据出境的技术和管理能力；</p> <p>数据接收方的安全保护能力、采取的措施；</p> <p>数据接收方所在国家或区域的政治法律环境。</p>	

## 第四节 监督管理与法律责任

### 一、监督管理

《网络安全法》第八条确定了数据本地化制度的管理体制为国家网信部门负责统筹协调网络安全工作和相关监督管理工作。国务院电信主管部门、公安部门和其他有关机关依照本法和有关法律、行政法规的规定，在各自职责范围内负责网络安全保护和监督管理工作。这就为执法和监督检查等活动的主体提供了明确的指引，并且定期检查能够有效地遏制企业不规范的自行评估行为，避免出现类似美欧安全港协定中多依靠企业自觉遵从，而管理部门监管无力的状况。

在《办法》中对于这种管理体制也有所体现，包括第五条国家网信部门统筹协调数据出境安全评估工作，指导行业主管或监管部门组织开展数据出境安全评估，以及第六条中行业主管或监管部门负责本行业数据出境安全评估工作，定期组织开展本行业数据出境安全检查，以及在第九条中行业主管或监管部门不明确的，由国家网信部门组织评估。将国家网信部门作为监管的最后一道屏障，将有效避免多头监管或监管空白情况的出现，也为网络运营者的法规遵从等环节提供保障。

### 二、法律责任

对于一项完善的法律制度而言，需要规定相应的法律责任以从反面保障制度的落实，数据本地化制度也不例外。对网络运营者法律责任而言，主要体现为：《办法》第十四条，即“违反本办法规定的，依照有关法律法规进行处罚”；《网络安全法》第六十六条，即“关键信息基础设施的运营者违反本法第三十七条规定，在境外存储网络数据，或者向境外提供网络数据的，由有关主管部门责令改正，给予警告，没收违法所得，处五万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照；

对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款”。从法律规定可以看出，国家对于违反数据本地化政策的处罚较为严厉，暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照将对网络运营者的生产经营活动造成直接的影响，对于企业形象和社会声誉也是不小的打击，这也可以从反面保障法律规定的切实执行。

总而言之，我国的数据本地化政策填补了对于数据跨境流动方面的制度空白，满足了现阶段我国网络社会治理的迫切需求。截至目前，《网络安全法》、《个人信息和重要数据出境安全评估办法（征求意见稿）》、《信息安全技术 数据出境安全评估指南（草案）》的相继出台和发布，说明数据本地化政策的贯彻落实已经成为必然。因此，作为法律法规落实的重要环节，网络运营者应在贯彻安全与发展平衡原则的基础上，对法律遵从提前进行预判，将数据本地化制度落到实处。除此之外，数据本地化政策以及安全评估制度都赋予企业新的义务，将不可避免地增加企业运营成本，网络运营者在落实过程中，也应正确处理增加的成本以及带来的安全性之间的平衡，不可偏废其一，从而违背立法本意。

## 第 17 章

# 网络安全信息共享

全球化融合态势下，网络威胁信息成为关键信息基础设施安全保护的关键要素，及时共享和分析有价值的网络威胁信息已被视为新技术背景下提升关键信息基础设施安全保护能力的重要内容。2016 年 4 月 19 日，习近平总书记在网络安全和信息化工作座谈会上明确提出，要全天候全方位感知网络安全态势，要建立统一高效的网络安全风险报告机制、情报共享机制、研判处置机制，准确把握网络安全风险发生的规律、动向、趋势，要建立政府和企业网络安全信息共享机制。随后，《国家网络空间安全战略》明确提出，关键信息基础设施保护是政府、企业和社会的共同责任，要求建立政府、行业与企业的网络安全信息有序共享机制，充分发挥企业在保护关键信息基础设施中的重要作用。同时，《网络空间国际合作战略》指出，加强国际合作，提升保护关键信息基础设施的意识，推动建立政府、行业与企业的网络安全信息有序共享机制，加强关键信息基础设施及其重要数据的安全防护。由此可见，我国已将关键信息基础设施安全保护领域的网络安全信息共享上升至国家战略的高度。

在立法层面，我国也逐步认识到加强网络安全信息共享对于实现关键信息基础设施安全保障的必要性和迫切性。在延续《网络安全法（草案一次审议稿）》和《网络安全法（草案二次审议稿）》相关规定的基础上，正式公布的《网络安全法》在第三十九条第三款再一次明确提出了关键信息基础设施保护领域的网络安全信息共享，其中要求国家网信部门统筹协调有关部门、关键信息基础设施的运营者，

以及有关研究机构、网络安全服务机构等之间的网络安全信息共享。同时,《关键信息基础设施安全保护条例(征求意见稿)》第三十八条也要求国家网信部门统筹协调有关部门、运营者,以及有关研究机构、网络安全服务机构建立关键信息基础设施网络安全信息共享机制,促进网络安全信息共享。由此表明我国关键信息基础设施保护领域的网络安全信息共享已迈入法治化进程。

## 第一节 《网络安全法》相关规定及释义

### 一、网络安全信息共享的范围界定

《网络安全法》第二十六条通过列举方式界定了网络安全信息共享的范围——网络安全信息,包括系统漏洞、计算机病毒、网络攻击、网络侵入等,这是从网络安全信息的技术类型角度所做出的定义,体现了网络安全信息承载网络安全风险的基本功能。上述规定的系统漏洞、计算机病毒、网络攻击、网络侵入等与关键信息基础设施保护相关的网络安全信息都应当属于网络安全信息共享的范围。基于此,从网络安全基本法层面概括界定网络安全信息共享的范围,能够为制定相应的配套规定和网络安全信息共享指南等技术标准提供法律依据。

具体而言,网络安全信息共享的范围应当包括以下几类。①关键信息基础设施的安全事件信息:关于成功的或未遂的针对关键信息基础设施的网络攻击的细节信息,具体包括丢失的信息、攻击中使用的技术、攻击意图、造成的影响等。②针对关键信息基础设施的网络威胁信息:包括尚未认识清楚但可导致潜在严重影响的事项;感染指标(Indicators of Compromise, IoC),如恶意文件、被窃取电子邮箱地址、受影响的IP地址、恶意代码样本;关于威胁实施者的信息。该类信息有助于发现安全事件,从攻击中吸取教训,创造解决方案等。③关键信息基础设施的漏洞信息:支撑关键信息基础设施运行的软件、硬件、商业流程中可被恶意利用的漏洞。④缓解措施信息:包括修补关键信息基础设施漏洞、封阻或遏制威胁、安全事件响应和恢复的方法。此类信息一般以漏洞补丁、杀毒软件升级

等形式存在。⑤态势感知信息：此类信息包括对被利用漏洞、活跃的威胁、攻击的实时遥测，还包括攻击目标、网络状况等信息，能够帮助决策人员响应安全事件。⑥最佳实践：关于关键信息基础设施的安全产品和服务的开发和部署的信息，包括安全控制、时间响应流程、软件漏洞修补等。⑦战略分析：综合、提炼、分析来自各方面的信息，以构建度量体系、描绘趋势、开展预测，帮助政府和企业决策者为未来的风险提前做准备<sup>①</sup>。

然而，值得注意的是，共享的网络安全信息应当是对于描述或识别关键信息基础设施的网络安全威胁而言必要的信息，这就要求不得共享与网络安全威胁不直接相关的个人信息或可识别特定个人的任何信息，例如健康医疗信息、人力资源信息、购买偏好、教育背景、信用信息等，此类信息属于网络安全信息共享的除外范围。举例说明，针对关键信息基础设施运营者内部员工的钓鱼电子邮件而言，有关电子邮件发件人（“From” / “Sender” 地址）的个人信息，电子邮件中的恶意 URL，附加在电子邮件中的恶意软件文件，电子邮件的内容，以及与恶意电子邮件或潜在的网络安全威胁行为相关的其他电子邮件信息，如主题行，消息 ID 和 X-Mailer，都可能被认为与网络安全威胁直接相关。然而，目标电子邮件的姓名和电子邮件地址（即“To” 地址）是与网络安全威胁无直接关系的个人信息，因此通常不应将其作为网络威胁指标的一部分而被共享。然而，个人可识别信息（Personally Identifiable Information, PII）或个人信息很可能偶然地对于描述针对关键信息基础设施的网络安全威胁或防御性措施而言十分必要，在此情况下，其应当属于网络安全信息共享的范围。

## 二、网络安全信息共享的参与主体

《网络安全法》第三十九条第三款明确规定了关键信息基础设施保护领域的网络安全信息共享参与主体，包括国家网信部门、有关部门、关键信息基础设施的运营者，以及有关研究机构、网络安全服务机构等。此外，《关键信息基础设施安全保护条例（征求意见稿）》第三十八条再次确定了与《网络安全法》上述规定保

---

① Cristin Goodwin, J. Paul Nicholas. A framework for cybersecurity information sharing and risk reduction[R/OL]. [2015-10-10]. <https://www.microsoft.com/en-us/download/details.aspx?id=45516>.

持一致的网络安全信息共享参与主体的范围。其中，有关部门通常是指关键信息基础设施所属行业的主管或监管部门，包括公安、工信、国家安全、国家保密行政管理、国家密码管理等部门。由此可见，网络安全信息共享的参与主体非常广泛，包括政府有关部门、关键信息基础设施的运营者、有关研究机构、网络安全服务机构，以及受网络安全威胁影响的相关企业等。

### 三、网络安全信息共享参与主体的法律责任及其豁免规定

#### （一）网络安全信息共享参与主体的法律责任

关键信息基础设施作为保障国家安全和社会持续运转的重要支撑，围绕关键信息基础设施安全保护的网络安全信息共享将在《网络安全法》的相关配套规定中逐渐凸显出强制性的特征，即关键信息基础设施的所有或运营企业必须与政府有关部门，以及其他具有依赖性的关键信息基础设施运营者之间进行有关系统漏洞、网络入侵、攻击、预警和应对策略等关键信息基础设施网络安全相关信息的及时交换。不履行共享义务导致严重网络安全危害后果，或违反共享相关要求的应当承担法律责任。

此外，对于企业一方在信息共享的过程中不当泄露国家机密、商业秘密，没有采取安全防护措施导致其接收的共享信息被未经授权地访问，以及并未采取技术措施移除接收的个人可识别信息导致个人隐私受到侵犯的，应当依据《国家安全法》、《保密法》、《刑法》、《民法》、《全国人民代表大会常务委员会关于加强网络信息保护的决定》等相关法律法规的规定承担相应的法律责任。法律责任的认定标准基于参与主体的主观目的，即政府有关部门和关键信息基础设施所有或运营企业基于主观善意实施网络安全信息共享相关法律法规授权的行为应当受到法律保护，但是，双方在网络安全信息共享的过程中基于故意或重大过失导致侵权的，应当承担相应的法律责任。

#### （二）网络安全信息共享参与主体的法律责任豁免规定

网络安全信息共享的制度设计更多地将焦点集中于参与信息共享的关键信息



基础设施运营企业的法律责任豁免方面，因为在实践中企业拥有关于信息系统漏洞、黑客、补丁和事件响应的有价值信息，如果其不清楚这些信息将被如何用于加强网络安全，或其担心上述信息是敏感信息，则其通常不愿意共享这些信息。尤其是在大数据时代背景下，数据来源的广泛性将直接导致企业面临数据来源的合法性举证难题，从法律责任追究的角度来看，企业通常认为其持有网络威胁信息比互利共享信息更加安全。因此，通过法律法规为关键信息基础设施运营企业与政府有关部门共享网络安全信息设定明确的法律责任豁免规则，能够提高企业参与网络安全信息共享的积极性，充分发挥其在应对关键信息基础设施的网络安全威胁中的重要作用。

具体而言，网络安全信息共享参与主体的法律责任豁免主要包括反垄断责任豁免和信息公开豁免两个方面。首先，我国《反垄断法》第十三条规定，禁止具有竞争关系的经营者达成下列垄断协议：①固定或者变更商品价格；②限制商品的生产数量或者销售数量；③分割销售市场或者原材料采购市场；④限制购买新技术、新设备或者限制开发新技术、新产品；⑤联合抵制交易；⑥国务院反垄断执法机构认定的其他垄断协议。然而，网络安全信息共享参与主体之间进行的信息共享行为不具有排除、限制竞争的效果，没有违反《反垄断法》的相关规定，因此，按照法律法规的要求参与网络安全信息共享的主体不应当承担《反垄断法》针对垄断行为设定的法律责任。其次，参与网络安全信息共享的关键信息基础设施运营企业享有《政府信息公开条例》的信息公开豁免权利。一般而言，企业可能担心其系统漏洞或面临的网络安全威胁是敏感信息而不愿意向公众披露，因为这一披露可能导致企业面临商业秘密泄露、名誉受损、竞争劣势、利润损失、股东派生诉讼和其他诉讼，以及政府有关部门滥用共享信息等困境。我国《政府信息公开条例》第十四条第四款规定，行政机关不得公开涉及国家秘密、商业秘密、个人隐私的政府信息。基于此，为了激励企业与政府有关部门共享关键信息基础设施的网络威胁信息，关键信息基础设施运营企业共享给政府有关部门的关键信息基础设施网络安全信息应当基于上述公众披露的豁免规定可免于向公众披露。

## 四、网络安全信息共享的程序规范

### （一）对接收的共享信息进行全面审查

在网络安全信息共享的过程中，政府有关部门和关键信息基础设施运营企业均应当采取措施对其获取和接收的网络安全信息进行审查，及时销毁与网络安全威胁没有直接关系的特定个人信息或个人可识别信息（PII）。更为重要的是，针对共享信息的政府有关部门或关键信息基础设施运营企业接收主体而言，如果其明知共享的信息存在错误，则其有义务向国家网信部门、政府有关部门，以及其他已确定的信息共享参与主体进行书面通知，避免造成不必要的损害。同时，国家网信部门和政府有关部门应当及时通知该错误信息的原始发送者并责令其停止传输该错误信息，尽快删除或更新信息。共享参与主体因错误共享信息而导致相关主体权益受损的，应当根据其在接收信息时是否知情及是否及时有效地采取了相应的补救措施来判定其是否应当承担相应的法律责任。

### （二）保障共享信息的存储安全

在网络安全信息共享的过程中，政府有关部门和关键信息基础设施运营企业存储其接收的网络安全信息也应当履行相应的义务。第一，确定共享信息的存留期限，因为网络安全威胁随着时间的推移而发生变化，有时几乎与威胁的确定保持同步。因此，网络安全信息的有用性和及时性可能限制在短时间内。为了减轻陈旧或质量差的信息的使用，网络安全信息只保留一段特定的时间，或直到与法律授权的使用目的不再直接相关时进行删除。第二，采取安全防护措施，以保护那些包含与网络安全威胁直接相关的特定个人信息或 PII 不受未经授权的访问或获取。上述安全防护措施具体包括内部用户访问控制，相关数据的物理或逻辑隔离，针对负责具体落实共享流程的政府官员和企业雇员进行网络安全培训，遵守《全国人民代表大会常务委员会关于加强网络信息保护的決定》、《信息安全技术公共及商用服务信息系统个人信息保护指南》等有关个人信息处理的目的明确原则、公开透明原则、质量保证原则、安全保障原则、合

理处置原则、知情同意原则。第三，政府有关部门和企业均应当采取措施对其获取和接收的网络安全信息进行审查，及时销毁与网络安全威胁没有直接关系的特定个人信息或个人可识别信息。

### （三）限制共享信息的非法使用

《网络安全法》原则性地限定了政府有关部门使用网络安全信息的目的。为了避免政府有关部门在网络安全信息共享的实施过程中滥用职权，不当获取、披露、存留和使用其获取的网络安全信息，《网络安全法（草案二次审议稿）》第三十八条明确规定，国家网信部门和政府有关部门，尤其是国家关键信息基础设施的行业主管或监管部门在关键信息基础设施保护中获取的信息，只能用于维护网络安全的需要，不得用于其他用途。针对这一规定，在正式公布的《网络安全法》第三章“网络运行安全”之“一般规定”的第三十条做出了扩大的限制性规定，即要求网信部门和有关部门在履行网络安全保护职责中获取的信息，只能用于维护网络安全的需要，不得用于其他用途，而不再仅仅局限于关键信息基础设施安全保护领域。例如，政府有关部门在共享过程中获得的信息不得用于行政执法中的证据，不得基于《政府信息公开条例》的披露义务向公众披露等，这一原则性限定与现有法律，如《行政诉讼法》、《政府信息公开条例》等能够进行有效衔接。

针对参与共享的企业如何使用其获取的网络安全信息，我国并未做出明确的限制性规定，但是，基于保护国家机密、企业商业秘密，以及个人隐私的实际需求，企业共享、接收或使用网络威胁信息只能基于维护网络安全的目的，即保护信息系统的机密性、完整性和可用性，确保系统及其中存储、处理和传输的信息免受网络安全威胁的影响。此外，在网络安全信息的使用与网络安全目的不再相关时，共享参与主体应当立即删除或销毁该信息。

### （四）传输前的共享信息审查

政府有关部门和关键信息基础设施运营者在传输网络安全信息之前应当主动实施人工或技术措施实施审查，审查内容包括：①该信息与网络安全威胁是否存在直接关联；②该信息是否包含特定个人信息或个人可识别信息。通过审查评估

以确定是否有必要采取适当的技术措施移除与网络安全威胁不直接相关的特定个人信息或个人可识别信息。此外，为了最大限度地保护涵盖特定个人信息或个人可识别信息网络安全信息的机密性，政府有关部门和企业应当告知共享信息的接收者仅可在法律授权的目的范围内使用此类信息。

## 第二节 网络安全信息共享制度概述

### 一、网络安全信息共享的概念界定

网络安全信息共享（Cybersecurity Information Sharing）这一概念最早由美国于 20 世纪 90 年代后期提出，涵盖国家之间，国内各级政府之间，政府与私有企业之间，以及私有企业相互之间的信息共享<sup>①</sup>。在美国，网络安全信息共享自提出之日起便与关键（信息）基础设施保护存在密切联系，由于美国大多数关键（信息）基础设施由私有企业所有并运营，所以美国政府持续关注政府有关部门和关键（信息）基础设施的运营企业之间网络安全信息共享机制的建立与完善，旨在通过一种自愿的、双向的、及时的网络安全信息交换，实现双方在网络安全风险识别、风险评估、风险预防 and 风险控制环节的技术能力和资源优势<sup>②</sup>。

基于各国对网络安全信息共享的关注焦点和政策立法趋势，以及我国关键信息基础设施安全保护的迫切需求，本章涉及的“网络安全信息共享”主要是指，为了保障关键信息基础设施的安全，政府和企业，以及企业相互之间有关关键信息基础设施的技术漏洞、网络入侵、恶意攻击的技术细节，预警信息和应对策略等网络安全相关信息的及时交换、沟通与交流。由此可见，关键信息基础设施保护领域的网络安全信息共享贯穿网络安全风险识别、评估、预防和控制的全过程，同时具有信息交换双向性和及时性的特点。

① 马民虎. 信息安全法研究[M]. 西安：陕西人民出版社，2004.

② Gregory T. Nojeim. Cybersecurity and Freedom on the Internet[J]. Journal of National Security Law & Policy, 2010(4):119-137.

## 二、美国关于网络安全信息共享范围的界定

美国 2015 年《网络安全信息共享法》(Cybersecurity Information Sharing Act of 2015, CISA)<sup>①</sup>规定,网络安全信息共享的范围必须与网络安全威胁直接相关,包括网络威胁指标(Cyber Threat Indicator)和防御性措施(Defensive Measure)两大类。其中网络威胁指标是指“对于描述或识别下列网络数据而言必要的信息,即:①恶意扫描探测,包括异常模式的通信,其目的旨在收集与网络安全威胁或安全漏洞相关的技术信息;②破坏安全控制措施或者利用安全漏洞的方法;③安全漏洞,包括表明存在安全漏洞的异常活动;④导致用户在对信息系统或其中存储、处理或传输的信息进行合法访问时不经意地破坏安全控制措施的方法;⑤恶意的网络命令和控制;⑥事件造成的实际或潜在的损害(包括因描述网络安全威胁而引发的信息泄露);⑦网络安全威胁的其他特性,如果披露该特性不被法律另行禁止。同时,防御性措施被界定为“以信息系统及其中存储、处理或传输的信息为保护对象,所采用的用于防止、减轻已知或可疑的网络安全威胁或安全漏洞的行动、设备、程序、签名、技术或其他措施,但不包括对信息系统或其中存储、处理或传输的信息进行破坏、销毁、提供未经授权的访问或造成实质性损害的措施”。

美国国土安全部和司法部于 2016 年联合发布的《根据 2015 年〈网络安全信息共享法〉协助非联邦实体与联邦实体共享网络威胁指标和防御性措施的指导意见》(以下简称《指导意见》,Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under the Cyber Security Information Sharing Act of 2015)<sup>②</sup>针对网络安全信息共享的范围做出了进一步的界定和举例说明,从而为参与共享的企业提供了明确的实施指引。其中指出,网络威胁指标的共享实例包括:①公司报告其 Web 服务器日志文件,其中显示特定的已发送 Web 流量的 IP 地址,以测试该公司的内容管理系统是否尚未更新以弥补最新漏洞;②安全研究人员可以报告其发现的允许未经授权访问工业控制系统的技

① 参考 <https://www.justsecurity.org/wp-content/uploads/2015/12/Cybersecurity-Act-of-2015.pdf>。

② 参考 <https://www.us-cert.gov/ais>。

术；③软件发布者可以报告其在其软件中发现的漏洞；④安全服务公司可以报告其认为对应恶意软件感染的域名查找模式；⑤制造商可以报告在其网络上发现的未执行的恶意软件；⑥研究人员可以报告与僵尸网络命令和控制服务器相关的域名或 IP 地址；⑦遭到计算机入侵的工程公司可以描述已被泄露的工程文件的类型，作为对其他拥有类似资产的公司的一种警告方式；⑧遭到分布式拒绝服务攻击其网站的报纸可以报告发送恶意流量的 IP 地址。

《指导意见》还规定，防御性措施可能像保护或限制访问公司计算机基础设施的安全装置一样简单，也可能像检测和防范公司信息系统上的异常和未经授权的活动而使用的复杂的软件工具一样复杂。与网络威胁指标类似，防御性措施也不包括个人信息或 PII，其由能够用于检测或应对网络安全威胁的技术信息构成。防御性措施的实例包括：①用于识别流入一个组织的网络流量中的恶意活动模式的计算机程序；②为了检测具有特定特征的钓鱼活动可以加载到公司入侵检测系统中的签名；③禁止一种恶意流量进入网络的防火墙规则；④可以通过网络流量缓存搜索来发现可能表示恶意活动的异常模式的算法；⑤一种以自动方式快速匹配组织传入的简单邮件传输协议（Simple Mail Transfer Protocol, SMTP，通常用于电子邮件的协议）内容的技术。

此外，《指导意见》还列举了受到美国其他可适用的隐私法保护的不直接与网络安全威胁相关的信息，即网络安全信息共享的除外范围，主要包括以下内容。

①受保护的健康信息（Protected Health Information, PHI），例如医疗记录、实验室报告或医院账单等，包括与个人的过去、现在或未来的身体或精神健康状况相关的信息；向个人提供医疗保健的信息；向个人提供医疗保健的过去、现在或未来的付款信息，因为每个文档将包含与健康数据内容相关联的患者姓名和/或其他识别信息。②人力资源信息，即员工人事档案中包含的信息，如招聘决策、绩效评估和纪律处分。③消费者信息/历史，即与个人购买、偏好、投诉甚至信用相关的信息。④教育历史，如成绩单、培训、专业认证等。⑤财务信息，包括银行报表、贷款信息、信用报告等。美国《格雷姆—里奇—比利雷法案》（Gramm-Leach-Bliley Act, GLBA），要求金融机构为消费者提供金融产品或服务，如贷款、金融或投资咨询或保险的公司应当向其用户解释其信息共享实践并保护用户的敏感数据。⑥确定有关财产所有权的信息，虽然关于财产所有权的一些信息可能是公开

的，例如物业购买记录，但其他信息如车辆识别号码本身就更加敏感，通常由州法律管辖。<sup>⑦</sup>识别 13 岁以下儿童的信息受《儿童在线隐私保护法》（Online Privacy Protection Act, COPPA）的一些要求的约束。美国 2015 年《网络安全信息共享法》界定的共享信息范围如图 17-1 所示。

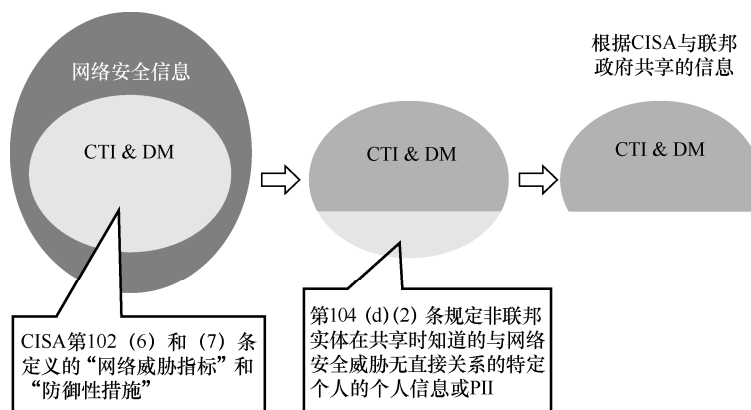


图 17-1 美国 2015 年《网络安全信息共享法》界定的共享信息范围

### 三、美国网络安全信息共享参与主体的法律责任豁免规定

美国政府充分认识到在其现有法律法规的框架下建立网络安全信息共享激励机制的必要性，当对于网络安全信息的共享必要且适当时应设置对企业有限的免责条款，促使产业自身利益，而非强制实施政府命令来驱动信息共享，具体的法律责任豁免规定包括反垄断责任豁免、知识产权保护和公众披露豁免、法律责任豁免。

首先，美国网络安全信息共享的法律障碍涉及反垄断法的规定，从法律责任追究的角度来看，私有企业通常认为其持有网络威胁信息比互利共享信息更加安全，因为美国的反垄断法禁止签订各种导致贸易限制或引发商业竞争者之间相互勾结的协议<sup>①</sup>。为了鼓励私有企业积极参与网络安全信息共享，美国司法部和联邦贸易委员会于 2014 年 4 月发布了一份关于信息共享和反垄断的联合政策声明，其

<sup>①</sup> Congressional Research Service. Cybersecurity Selected Legal Issues [R/OL].[2013-7-20]. <http://www2gwu.edu/~nsarchiv/NSAEBB/.../docs/Cyber-067.pdf>.

中明确指出，参与网络安全信息共享的机制不同于反垄断法禁止的掠夺性定价，竞争者市场分割，垄断或试图垄断，拒绝交易，交换价格、成本、客户名单或未来竞争计划信息的行为<sup>①</sup>，因此，网络安全信息共享不被视为可能引发反垄断问题。此外，美国 2015 年《网络安全信息共享法》进一步从法律层面确立了反垄断豁免机制，其中规定，基于保障网络安全的目的，两个或两个以上的私有实体之间交换或提供网络威胁指标或防御性措施，或协助预防、调查、减轻网络威胁的行为不应被认定为违反反垄断法的行为。然而，这一激励机制的适用范围有所限定，即交换信息或提供协助仅仅是为了实现下列目的：协助防止、调查或减轻针对信息系统或系统中存储、处理或传输的信息免受网络安全威胁的影响；协助传播或披露网络威胁指标以帮助防止、调查或减轻针对信息系统或系统中存储、处理或传输的信息免受网络安全威胁的影响。

其次，根据美国《信息自由法》（Freedom of Information Act, FOIA）的规定，向政府提供的信息应当向公众披露。然而，私有企业可能担心其系统漏洞或面临的网络安全威胁是敏感信息而不愿意向公众竞争者披露其专有文档和信息，因为这一披露可能导致私有企业面临商业秘密泄露、名誉受损、竞争劣势、利润损失、股东派生诉讼和其他诉讼等困境。基于此，为了激励私有企业与联邦政府共享网络威胁信息，美国以法律条文的形式明确规定，私有企业向联邦政府机构提供的网络威胁指标或防御性措施应被视为该私有企业的商业、金融和专有信息，因此，私有企业与政府共享网络威胁指标和防御性措施的行为不当视为放弃对其自身知识产权或商业秘密的保护。<sup>②</sup>同时，企业自愿共享给政府的网络威胁指标和防御性措施基于公众披露豁免规定可免于向公众披露。美国国土安全部和司法部于 2016 年联合发布的《根据 2015 年〈网络安全信息共享法〉协助非联邦实体与联邦实体共享网络威胁指标和防御性措施的指导意见》（Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under the Cybersecurity Information Sharing Act of 2015）进一步规

---

① Department of Justice, Federal Trade Commission. Antitrust Policy Statement on Sharing of Cybersecurity Information[EB/OL].[2014-8-25]. [https://www.ftc.gov/system/files/documents/public\\_statements/297681/140410ftcdojcyberthreatstmt.pdf](https://www.ftc.gov/system/files/documents/public_statements/297681/140410ftcdojcyberthreatstmt.pdf).

② Paul Rosenzweig. Cybersecurity Information Sharing One Step Toward U.S. Security, Prosperity, and Freedom in Cyberspace[R/OL]. [2014-4-2]. <http://www.heritage.org/research/reports/2014/04/cybersecurity-information-sharing-one-step-toward-us-security-prosperity-and-freedom-in-cyberspace>.



定,根据 2015 年《网络安全信息共享法》共享的网络威胁指标和防御性措施不受联邦国家,部落或地方政府信息自由法律,公开的政府法律,公开会议法,公开记录法,阳光法,或需要披露信息或记录的类似法律规制。

再次,基于网络安全目的,私有企业监控信息系统的行为适用法律责任豁免规定。私有企业监控其自身的信息系统;在经过其他实体授权和书面同意的情况下,监控其他实体的信息系统;在经过联邦实体有权代表的授权和书面同意的情况下,监控联邦实体的信息系统;监控上述信息系统中存储、处理或传输的信息的行为不被追究法律责任<sup>①</sup>。另外,私有企业共享或接收网络威胁指标的行为适用法律责任豁免规定。私有企业基于网络安全目的,并遵守机密信息的保护规定,与其他非联邦实体或联邦政府共享或接收网络威胁指标和防御性措施的行为不被追究法律责任<sup>②</sup>。

最后,美国的网络安全信息共享不强制私有企业与联邦政府共享网络威胁指标或防御性措施,也不强制私有企业在接收网络威胁指标或防御性措施的情形下进行预警或采取行动。一般情况下,联邦政府无权要求私有企业向联邦政府或其他私有企业提供信息;或以共享网络威胁指标为条件,要求私有企业向联邦政府或其他私有企业提供网络威胁指标;或以联邦补助金、合同、政府采购为条件,要求私有企业向联邦政府或其他私有企业提供网络威胁指标。此外,选择不参加自愿共享行为的实体不承担任何法律责任。

## 四、美国网络安全信息共享的组织机构及其职责

美国国土安全部及其分支机构(具体工作由国家保护和计划司承担)主要负责调整体的网络安全信息共享事项,国家情报总监办公室(具体工作由网络威胁和情报整合中心承担)负责有关共享网络威胁情报的分析工作。同时,美国各州、地方、部落和区域政府之间及其与联邦政府机构之间通过一个跨州的信息共享与分析中心促进公共与私有部门之间的信息共享。目前,美国各关键部门(行

① Melanie J. Teplinsky. Fiddling on the Roof Recent Developments in Cybersecurity[J]. American University Business Law Review, 2013(2): 225-322.

② Brian B. Kelly. Investing in a Centralized Cybersecurity Infrastructure: Why“Hacktivism” Can and Should Influence Cybersecurity Reform[J]. Boston University Law Review, 2012, (92):1663-1711.

业)，如金融、能源、通信、交通等已经建立了 18 个基于行业的信息共享与分析中心（Information Sharing and Analysis Centers, ISACs），负责协调、促进各行业内部公共与私有部门之间的网络安全信息共享；非关键部门的企业也通过建立并加入非行业性的信息共享与分析组织（ISAOs），进一步完善网络安全信息共享的机构体系。由此可见，美国已经建立了包括联邦政府机构、各地区、各行业分工配合的网络安全信息共享组织机构体系，其中最具有代表性的机构为 NCCIC、CTIIC、ISACs 和 ISAOs，并且其相互之间能够实现网络安全信息共享职能分工的补充和整合。

### （一）国家网络安全和通讯整合中心

2009 年 10 月，国土安全部内部建立了国家网络安全和通信整合中心（National Cybersecurity and Communications Integration Center, NCCIC），作为隶属于国家保护和计划司（National Protection and Programs Directorate, NPPD）的网络安全和通信办公室（Office of Cybersecurity and Communications, CS&C）的五大分支机构之一，NCCIC 负责有关网络安全信息共享事项，是一个 24×7 小时的网络态势感知、事件响应和管理中心，为联邦政府、情报机构和执法机关提供网络和通信整合的国家连接点，其在公共和私有部门之间共享有关漏洞、入侵、事件、风险减轻措施和恢复活动的信息。NCCIC 由 NCCIC 运行和整合中心（NCCIC Operations and Integration, NO&I）、US-CERT、ICS-CERT 和国家通信协调中心（National Coordinating Center for Communications, NCC）组成。

NCCIC 负责的与网络安全信息共享相关的职责包括：①作为美国跨部门的网络安全信息共享平台；②协调跨联邦政府的网络安全风险和事件的信息共享；③针对收集的网络安全信息进行整合和分析，包括跨部门的一体化网络安全风险和事件分析，并与联邦和非联邦实体共享分析结果；④向联邦或非联邦实体的网络安全风险或事件提供及时的技术协助、风险管理支持，以及事件响应能力，包括分析事件原因，共享缓解和补救措施；⑤向联邦和非联邦实体提供安全和权宜措施的信息和建议，特别是包括促进信息安全、加强信息系统应对网络安全风险的信息和建议。

## （二）网络威胁与情报整合中心

2015 年 2 月,美国总统奥巴马要求国家情报总监(Director of National Intelligence, DNI)成立网络威胁与情报整合中心(Cyber Threat Intelligence Integration Center, CTIIC),该机构将协调整合国土安全部、联邦调查局、中央情报局、国家安全局等多部门的情报力量,提高美国防范和应当网络攻击的能力,该机构将成为美国政府防范和应对网络威胁的主要部门及全国性的网络威胁情报中枢。

## （三）信息共享与分析中心

特定的关键部门的信息共享与分析中心是非营利性的,由关键基础设施的所有者和运营者基于成员关系形成的,在政府和企业之间共享信息的组织<sup>①</sup>。跨州的信息共享与分析中心(MS-ISAC)是国土安全部指定为各州、地方、部落和区域政府的网络安全 ISAC。

## （四）信息共享与分析组织

2015 年,奥巴马总统签署《改善私有领域网络安全信息共享行政令》,鼓励 ISAOs 的自愿形成和建立,其中包括非营利社区组织、会员组织或单一企业。ISAOs 的目标在于扩展当前的网络安全信息共享模型。与 ISACs 类似,ISAOs 的目的在于收集、分析和传播网络威胁信息,但与 ISACs 不同的是,ISAOs 并不基于具体行业而建立,使那些原本没有机会参与信息共享的实体加入其中。

# 五、美国网络安全信息共享的程序规范

美国 2015 年《网络安全信息共享法》规定,一方面,私有企业可以基于网络安全目的共享、接收或使用网络威胁信息;另一方面,联邦政府机构对其接收的网络威胁信息进行披露、存留和使用的目的仅限于:①网络安全目的;②识别网络安全威胁(包括此类网络安全威胁的来源)或安全漏洞;③识别国外敌对势力

---

<sup>①</sup> Sue Eckert. Protecting Critical Infrastructure: The Role of the Private Sector[J/OL]. [2014-1-20].[www.ridgway.pitt.edu/Portals/1/pdfs/Publications/Eckert.pdf](http://www.ridgway.pitt.edu/Portals/1/pdfs/Publications/Eckert.pdf).

或恐怖分子使用信息系统引发的网络安全威胁；④响应、减轻或防止因恐怖活动或使用大规模杀伤性武器而造成的死亡威胁，严重的人身伤害或经济损失；⑤响应、减轻或防止针对未成年人的严重威胁（包括性剥削和人身安全的威胁）；⑥阻止、调查或起诉特定的犯罪（包括严重的暴力犯罪，欺诈和身份盗用，间谍罪，以及侵犯商业秘密的犯罪）。

此外，美国国土安全部和司法部于 2016 年联合发布的《美国隐私和公民自由最终指南：2015 年网络安全信息共享法》（Privacy and Civil Liberties Final Guidelines: Cybersecurity Information Sharing Act of 2015）<sup>①</sup>重点规定了联邦实体接收、存留、使用和传输网络威胁指标的隐私和公民自由保护要求。

一方面，联邦实体接收、存留、使用和传输网络威胁指标应当遵守《联邦信息实践准则》有关信息的原则，具体包括以下内容。①透明原则。要求联邦实体根据 2015 年《网络安全信息共享法》在接收、存留、使用和传输网络威胁指标的过程应当是透明的；联邦实体应根据 2002 年《电子政务法》的规定完成和发布隐私合规文件，如隐私影响评估，并酌情制定机构内部的隐私政策，以充分描述其根据 2015 年《网络安全信息共享法》对网络威胁指标的接收、存留、使用和传输情况；并且联邦政府已经制定了向任何美国人及时通知联邦实体违反 2015 年《网络安全信息共享法》共享个人信息的程序。②目的明确原则。这一原则要求联邦政府机构接收、存留、使用和传输网络威胁指标仅限于网络安全目的，即保护信息系统及系统中存储、处理或传输的信息免受网络安全威胁或安全漏洞的影响。③数据最小化原则。这一原则要求联邦政府及时销毁其已知的与 2015 年《网络安全信息共享法》授权的相关用途不直接相关的包含特定个人信息或 PII 的网络威胁指标。④使用限制。这一原则要求联邦政府对其接收的网络威胁信息进行使用的目的仅限于上述 6 种情形。⑤数据质量和完整性。网络安全威胁随着时间的推移而发生变化，有时几乎与威胁的确定保持同步。因此，个人网络威胁指标的有用性和及时性可能限制在短时间内。为了避免使用过时或质量差的信息，网络威胁指标只能保留一段特定的时间，或直到其与 2015 年《网络安全信息共享法》授权的使用不再直接相关时进行删除或更新。⑥安全。联邦实体应遵循要求，以保

---

① 参考 <https://www.us-cert.gov/ais>。

护那些包含与网络安全威胁直接相关的特定个人信息或 PII，或通过 2015 年《网络安全信息共享法》授权使用的用户信息的网络威胁指标不受未经授权的访问或获取。违反上述规定，联邦政府官员、雇员或代理人的活动将受到法律的制裁。

联邦实体接收、存留、使用和传输网络威胁指标和防御性措施应当遵循以下规定。第一，在信息接收阶段，联邦实体必须及时删除确定与 2015 年《网络安全信息共享法》授权的用途无直接关系的特定个人信息或 PII；针对已知或确定为错误共享或违反 2015 年《网络安全信息共享法》规定的，联邦政府应当在可行的范围内尽快通知传输主体，从该联邦实体处接收网络威胁指标或防御性措施的其他联邦实体和非联邦实体，原始信息发送者及国土安全部，由国土安全部告知信息的原始发送者该信息是错误的并要求其更新或删除共享的错误信息。通知内容应当包括：①确定为网络威胁指标和防御性措施的信息；②确定错误或违反相关规定的信息；③与传输主体更正错误相关的其他信息。如果美国公民其个人信息被确定为违反 2015 年《网络安全信息共享法》的相关规定被共享，则对此知情的信息接收主体、传输主体等应当及时将这一情况通知该美国公民，并立即采取相应的补救措施或纠正措施，防止损害扩大化。

第二，在信息使用阶段，联邦政府使用共享信息存在特定的目的限制，即上文提及的六种情形。

第三，在信息存留阶段，联邦政府存留信息必须与使用的目的一致，并及时销毁或删除与网络安全威胁无直接关系的特定个人信息或 PII。同时，政府机构应当采取适当的安全防护措施，包括内部用户访问控制；数据的物理和/或逻辑隔离；遵循联邦信息安全现代化法规定的要求和 NIST 800-53 第 4 版规定的隐私保护要求，以保护那些包含与网络安全威胁直接相关的特定个人信息或 PII 或通过 2015 年《网络安全信息共享法》授权的使用的用户信息的网络威胁指标不受未经授权的访问或获取。

第四，在信息传输阶段，美国 2015 年《网络安全信息共享法》对参与网络安全信息共享的联邦政府和私有部门均设定了共享网络威胁指标之前的个人信息移除义务和程序，其中要求联邦政府和私有部门在共享网络威胁指标之前主动实施人工或技术审查措施，以评估此类网络威胁指标是否包含任何其在共享时可能“知道”的、与网络安全威胁不直接相关的个人信息或可识别特定个人的任何信息，

并采取适当的技术措施将其移除。为了对此进行监督，2015 年《网络安全信息共享法》规定了移除个人信息的独立报告，其中要求美国总审计长在法定的期限内向国会提交报告，详细说明联邦政府从网路威胁指标或防御性措施中移除个人信息所采取的行动，此类报告还应针对解决有关隐私和公民自由事项的政策、程序和指南的充分性进行评估。

第三节 网络安全信息共享法规遵从框架及建议

根据《网络安全法》和《关键信息基础设施保护条例（征求意见稿）》的相关规定，网络安全信息共享目前被界定为一种国家激励性措施和机制，不具有法律强制性。然而，随着总体国家安全观内涵的不断丰富，关键信息基础设施保护领域的网络安全信息共享将逐渐演变为关键信息基础设施运营企业的强制性义务，基于此，纳入关键信息基础设施安全保护制度体系的相关企业则应当对此予以重视，审慎考虑网络安全信息共享的法规遵从要求，表 17-1 梳理了网络安全信息共享的法规遵从框架。

表 17-1 网络安全信息共享法规遵从框架

法律名称	法律条款	法律规定
《网络安全法》	第二十六条	开展网络安全认证、检测、风险评估等活动，向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息，应当遵守国家有关规定
	第三十九条	国家网信部门应当统筹协调有关部门对关键信息基础设施的安全保护采取下列措施： （三）促进有关部门、关键信息基础设施的运营者，以及有关研究机构、网络安全服务机构等之间的网络安全信息共享
	第三十条	网信部门和有关部门在履行网络安全保护职责中获取的信息，只能用于维护网络安全的需要，不得用于其他用途
《关键信息基础设施安全保护条例（征求意见稿）》	第三十八条	国家网信部门统筹协调有关部门、运营者，以及有关研究机构、网络安全服务机构建立关键信息基础设施网络安全信息共享机制，促进网络安全信息共享
	第四十三条	有关部门，以及网络安全服务机构在关键信息基础设施安全检测评估中获取的信息，只能用于维护网络安全的需要，不得用于其他用途

续表

法律名称	法律条款	法律规定
《保守国家秘密法》	第三条	<p>一切国家机关、武装力量、政党、社会团体、企业事业单位和公民都有保守国家秘密的义务。</p> <p>任何危害国家秘密安全的行为，都必须受到法律追究</p>
《刑法》	第二百一十九条	<p>有下列侵犯商业秘密行为之一，给商业秘密的权利人造成重大损失的，处三年以下有期徒刑或者拘役，并处或者单处罚金；造成特别严重后果的，处三年以上七年以下有期徒刑，并处罚金：</p> <p>（一）以盗窃、利诱、胁迫或者其他不正当手段获取权利人的商业秘密的；</p> <p>（二）披露、使用或者允许他人使用以前项手段获取的权利人的商业秘密的；</p> <p>（三）违反约定或者违反权利人有关保守商业秘密的要求，披露、使用或者允许他人使用其所掌握的商业秘密的。</p> <p>明知或者应知前款所列行为，获取、使用或者披露他人的商业秘密的，以侵犯商业秘密论。</p> <p>本条所称商业秘密，是指不为公众所知悉，能为权利人带来经济利益，具有实用性并经权利人采取保密措施的技术信息和经营信息。</p> <p>本条所称权利人，是指商业秘密的所有人和经商业秘密所有人许可的商业秘密使用人</p>
	第二百五十三条	<p>违反国家有关规定，向他人出售或者提供公民个人信息，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。</p> <p>违反国家有关规定，将在履行职责或者提供服务过程中获得的公民个人信息，出售或者提供给他人的，依照前款的规定从重处罚</p>
《反不正当竞争法》	第十条	<p>经营者不得采用下列手段侵犯商业秘密：</p> <p>（一）以盗窃、利诱、胁迫或者其他不正当手段获取权利人的商业秘密；</p> <p>（二）披露、使用或者允许他人使用以前项手段获取权利人的商业秘密；</p> <p>（三）违反约定或者违反权利人有关保守商业秘密的要求，披露、使用或者允许他人使用其所掌握的商业秘密。第三人明知或者应知前款所列违法行为，获取、使用或者披露他人的商业秘密，视为侵犯商业秘密。本条所称的商业秘密，是指不为公众所知悉、能为权利人带来经济利益、具有实用性并经权利人采取保密措施的技术信息和经营信息</p>

续表

法律名称	法律条款	法律规定
《反不正当竞争法》	第二十五条	违反本法第十条规定侵犯商业秘密的，监督检查部门应当责令停止违法行为，可以根据情节处以一万元以上二十万元以下的罚款
《全国人大常委会关于加强网络信息保护的决定》	(二)	网络服务提供者和其他企业事业单位在业务活动中收集、使用公民个人电子信息，应当遵循合法、正当、必要的原则，明示收集、使用信息的目的、方式和范围，并经被收集者同意，不得违反法律、法规的规定和双方的约定收集、使用信息。 网络服务提供者和其他企业事业单位收集、使用公民个人电子信息，应当公开其收集、使用规则
	(三)	网络服务提供者和其他企业事业单位及其工作人员对在业务活动中收集的公民个人电子信息必须严格保密，不得泄露、篡改、毁损，不得出售或者非法向他人提供
	(四)	网络服务提供者和其他企业事业单位应当采取技术措施和其他必要措施，确保信息安全，防止在业务活动中收集的公民个人电子信息泄露、毁损、丢失。在发生或者可能发生信息泄露、毁损、丢失的情况时，应当立即采取补救措施
	(十)	国家机关及其工作人员对在履行职责中知悉的公民个人电子信息应当予以保密，不得泄露、篡改、毁损，不得出售或者非法向他人提供
	(十一)	对有违反本决定行为的，依法给予警告、罚款、没收违法所得、吊销许可证或者取消备案、关闭网站、禁止有关责任人员从事网络服务业务等处罚，记入社会信用档案并予以公布；构成违反治安管理行为的，依法给予治安管理处罚。构成犯罪的，依法追究刑事责任。侵害他人民事权益的，依法承担民事责任
《政府信息公开条例》	第十四条	行政机关不得公开涉及国家秘密、商业秘密、个人隐私的政府信息。但是，经权利人同意公开或者行政机关认为不公开可能对公共利益造成重大影响的涉及商业秘密、个人隐私的政府信息，可以予以公开
《互联网网络安全信息通报实施办法》	第二十三条	CNCERT 应与网络安全研究机构、网络安全技术支持单位、非经营性互联单位、网络安全企业、国际网络安全组织等广泛合作，积极拓展网络安全信息获取渠道

基于上述考虑，为了给政府和企业建立、参与网络安全信息共享关系提供指导，帮助企业设定信息共享目标、识别网络威胁信息源、确定信息共享活动范围、制定威胁信息发布与分发规则、加入现有共享组织、有效利用威胁信息，以支持



其总体网络安全实践，表 17-2 参照美国国家标准与技术研究院于 2016 年发布的《网络威胁信息共享指南》（Guide to Cyber Threat Information Sharing, NIST SP 800-150），通过梳理网络安全信息共享的控制项和法规遵从要求，以期帮助企业通过安全有效的信息共享实践来促进网络安全运营与风险管理活动，以及组织规划、实施与维护信息共享。

表 17-2 网络安全信息共享的法规遵从建议

控制项	网络安全信息共享的法规遵从建议	对应条款
共享信息的类型	<p>(1) 指标：可表明攻击即将或正在发生、或可能已出现入侵的技术因素（Technical Artifact）或可观察事件，包括可疑命令和控制（C&amp;C）服务器的 IP 地址、可疑 DNS 域名、引用恶意内容的 URL、恶意可执行文件的哈希值及恶意邮件的主题。</p> <p>(2) 策略、技术与过程（Strategy, Technology and Process, TTP）：指源起方行为。策略是对行为的概括描述，技术是对策略涉及行为的具体描述，过程是对技术的进一步、更详细的描述。从 TTP 可看出源起方倾向于使用何种恶意软件变种、运算顺序、攻击工具、传递机制（如钓鱼或水坑攻击）或攻击。</p> <p>(3) 安全警报：即公告（Advisory/Bulletin）和漏洞说明（Vulnerability Note），一般是对用户发布的有关现有漏洞、攻击及其他安全问题的简要技术通知。安全警报来源包括美国计算机紧急响应小组、信息共享与分析中心、国家漏洞库、产品安全事件响应小组、商业安全服务提供商、安全研究员等。</p> <p>(4) 威胁情报报告：一般用平实的语言写成，主要内容涉及 TTP、威胁源起方、目标系统与信息类型，以及使组织获得更高态势感知能力的其他威胁相关信息。威胁情报指汇总、转换、分析、解释或提炼后的威胁信息，为决策流程提供必要上下文。</p> <p>(5) 工具配置：对于搭建并使用工具（机制）提供的建议，这些工具（机制）为自动化采集、交换、处理、分析与使用威胁信息提供支持。工具配置信息可包括安装与使用 Rootkit 检测与清除工具、创建并定制入侵检测特征、路由器访问控制列表、防火墙规则或 Web 过滤配置文件等说明</p>	<p>第三十九条 国家网信部门应当统筹协调有关部门对关键信息基础设施的安全保护采取下列措施：</p> <p>（三）促进有关部门、关键信息基础设施的运营者以及有关研究机构、网络安全服务机构等之间的网络安全信息共享</p>
设定信息共享目标	<p>组织应制定目标，从组织的业务流程与安全政策方面，阐述信息共享的期望结果。这些目标有助于组织划定信息共享的工作范围，选择并加入共享社团，为信息共享活动提供持续支持</p>	

续表

控制项	网络安全信息共享的法规遵从建议	对应条款
设定信息共享目标	由于技术或资源的限制，可能需要为目标指定优先级，以保证要事先办	
识别内部现有的网络威胁信息源	<p>组织应识别当前收集、分析及存储的威胁信息，并确定如何使用信息，具体包括：</p> <ul style="list-style-type: none"> <li>● 确定生成威胁信息的传感器、工具、数据流及知识库，保证其生成的信息准确无误，生成频率满足要求，可充分支持网络安全决策；</li> <li>● 从收集并经过分析的安全信息中，找出用于组织持续监控策略的数据；</li> <li>● 从收集并储存的威胁信息中，找出可能没有进行持续分析或评审的数据（如操作系统默认审计日志文件）；</li> <li>● 查明哪些威胁信息适合与外界共享，以及哪些数据有助于高效响应网络威胁；</li> <li>● 识别组织内部威胁信息源的负责人及操作人</li> </ul>	
界定信息共享的活动范围	<p>组织应界定信息共享活动的范围，包括规定可共享的信息类型、信息共享的条件和对象。确定范围时，应判断哪类信息可经组织关键利益主体授权进行共享、此类信息在哪些情况下可进行共享，以及信息可以并应该共享给谁。</p> <p>组织信息共享活动的范围应与组织的资源、能力及目标相匹配。信息共享工作应聚焦于能为组织及其共享合作伙伴带来最大价值的活动</p>	
制定信息共享规则	<p>组织应制定信息共享规则，控制威胁信息发布和分发，防止传输敏感信息。信息共享规则应考虑到接收者的可信性、共享信息的敏感性，以及共享（或不共享）某类信息的潜在影响。</p> <p>在共享威胁信息前，组织应当：</p> <ul style="list-style-type: none"> <li>● 列出可能要共享的威胁信息类型；</li> <li>● 描述允许信息共享的条件和情况；</li> <li>● 确定已被批准的威胁信息接收人；</li> <li>● 描述编辑或筛选共享信息的要求；</li> <li>● 说明是否允许来源具名；</li> <li>● 应用信息处理标记，描述信息接收人的信息保护义务</li> </ul>	
定期重估组织的信息共享规则	<p>组织应当在发生下列安全事件时定期重估其信息共享规则：</p> <ul style="list-style-type: none"> <li>● 监管或法律要求发生变化；</li> <li>● 组织政策更新；</li> <li>● 引入新的信息源；</li> <li>● 风险容忍度发生变化；</li> <li>● 信息责任人发生变化；</li> <li>● 运营/威胁环境发生变化；</li> <li>● 组织兼并与收购</li> </ul>	

续表

控制项	网络安全信息共享的法规遵从建议	对应条款
保护个人隐私和敏感信息	<p>在处理网络威胁信息时可能涉及个人可识别信息、知识产权及商业秘密等敏感信息。这些信息若不当披露则会导致经济损失，违反法律、法规、合同，引起法律诉讼，或损害组织声誉。因此，组织应采取必要的安全与隐私控制措施及操作规程，如网络通信加密、认证和授权机制、知识库安全加固等，以保护个人可识别信息、知识产权、商业秘密等敏感信息不被非法泄露或修改。</p> <p>组织应制定具体的指导方案和流程，指导如何处理个人可识别信息等敏感信息</p>	
共享标记	<p>组织应仔细选择或者制定表示共享标记的方法，如采用流量指示灯协议（Traffic Light Protocol, TLP）。在 TLP 协议中，红色是指最严格的规则，琥珀色、绿色和白色所代表的规则依次宽松。</p> <p>当另一方不能有效响应信息，并且如果信息使用不当可能影响自己的隐私、名誉或运营时，信息共享组织可以使用红色标记，可共享的信息只能在特定的交流或会议范围内进行共享，共享信息的接收者不能将交流、会议或会话中透露的红色标记信息分享给与交流、会议或会话无关的任何其他组织。</p> <p>当信息需要支持以做出有效响应，但如果在组织外共享，可能有影响隐私、名誉或运营的风险时，信息共享组织可以使用琥珀色标记，共享信息的接收者可以与组织内部成员共享琥珀色标记的信息，但应根据响应需求控制范围。</p> <p>当信息有利于提高所有参与组织，以及更广泛的组织或行业同人的意识时，信息共享组织可以使用绿色标记，接收者可以与行业同人组织共享绿色标记的信息，但不会通过公开渠道共享。</p> <p>当按照公共发布的适用规则和流程，信息可预见的被滥用风险最小或者为零时，信息共享组织可以使用白色标记，白色标记的信息可以不受限制地分发，但受版权控制保护</p>	
加入共享组织	<p>组织应判断哪些共享活动可作为对现有威胁信息能力的补充，并积极参与这样的活动。</p> <p>为了满足运营需要，组织应当加入各种信息共享论坛，包括公共或私有组织、政府知识库（Repository）、商业网络威胁情报流，以及诸如公开网站、博客与数据流之类的公开源</p>	

续表

控制项	网络安全信息共享的法规遵从建议	对应条款
为信息共享活动提供持续支持	<p>组织应制订信息共享计划，为持续的基础设施维护与用户支持做准备。</p> <p>计划内容应包括如何收集、分析内外部威胁信息，以及在制定与部署防护措施时如何使用这些信息，方法应具有可持续性，以保证资源充分，能满足收集、存储、分析与传播网络威胁信息的需要</p>	
参与持续沟通	组织应持续参与共享活动并不断改进做法，如积极参与社团赞助的电话会议和面对面会议，以更好地建立与其他成员的信任关系，从而能够有效地合作	
主动制定网络威胁共享协议	组织应提前规划，在安全事件发生前制定共享协议，提前规划可确保参与组织明白其角色、职责与信息处理要求	
使用和响应安全警报	<p>一旦收到安全警报，组织应首先确定警报来源是否可信、可靠。当警报来自未知或不可信来源时，应当进行额外的审查或在采取行动前再次确认。如果警报被认为是可信的，组织应确定自己是否拥有或操作了任何在警报中列出的受影响的系统、应用程序或硬件；如果是，组织应做出恰当响应。</p> <p>在做出响应时，组织应通过评估警报的严重程度、组织内受影响系统的数量、攻击可能对组织关键职能的影响，以及部署缓解安全控制措施对操作的影响等因素，了解警报的整体影响。这一评估可为确定响应措施的优先级和具体方法提供参考。响应措施包括从告警中识别和提取指标、使用指标开发和部署检测特征、改变配置、应用补丁、通知威胁人员，以及实施或加强安全控制措施</p>	
利用自动化安全机制发布、使用、分析与响应网络威胁信息	组织应使用标准化数据格式与传输协议共享网络威胁信息，以简化威胁信息处理的自动化过程。使用自动化手段，可减少人为干预，快速共享、转换、丰富与分析网络威胁信息	
梳理与存储指标	<p>组织应采取合理措施确保使用合适的安全实践保护指标知识库，如限制访问，仅允许授权用户进行访问，定期备份知识库，维护知识库系统的操作系统和应用，安装当前补丁和采用安全配置，以及生产用于知识库的内部软件时采用软件开发最佳实践。</p> <p>组织应制定指标（通常还包括威胁信息）部署政策和规程。这些政策和规程应明确数据保留要求，以确保指标信息在短期（在线）和长期（离线）内可用。对于那些无须用作威胁证据的指标，组织应确定合理的保存政策</p>	

## 第四节 监督管理与法律责任

### 一、监督管理

我国《网络安全法》第三十九条明确规定国家网信部门是网络安全信息共享的主管机构，负责协调整体网络安全信息共享事项，其职责在于加强对政府和企业之间网络安全信息收集、分析和通报工作的指导、统筹和协调，按照规定统一发布网络威胁信息。第五十二条规定，负责关键信息基础设施安全保护工作的部门，应当建立健全本行业、本领域的网络安全监测预警和信息通报制度，并按照规定报送网络安全监测预警信息。《国家安全法》第五十一条规定，建立情报信息工作协调机制，实现情报信息的及时收集、准确研判、有效使用和共享。第五十二条规定，国家安全机关、公安机关、有关军事机关根据职责分工，依法搜集涉及国家安全的情报信息。《关键信息基础设施安全保护条例（征求意见稿）》第三十八条规定，国家网信部门统筹协调有关部门、运营者，以及有关研究机构、网络安全服务机构建立关键信息基础设施网络安全信息共享机制，促进网络安全信息共享。上述规定为网络安全信息共享工作的统筹协调和有效落实提供了组织机构保障。

具体而言，在国家网信部门的领导下，政府有关部门，包括公安、工信、国家安全、国家保密行政管理、国家密码管理等部门等应当在各自职责范围内负责落实网络安全信息共享工作的指导、协调和监督管理工作。值得注意的是，网络安全信息共享应当发挥我国军事机关和国家安全机关的重要作用，充分挖掘其在情报获取方面的独特优势和成熟经验。

### 二、法律责任

根据《网络安全法》和《关键信息基础设施保护条例（征求意见稿）》的相关

规定，网络安全信息共享目前被界定为一种国家激励性措施和机制，不具有法律强制性。然而，随着总体国家安全观内涵的不断丰富，关键信息基础设施保护领域的网络安全信息共享将逐渐演变为关键信息基础设施运营企业的强制性义务，基于此，纳入关键信息基础设施安全保护制度体系的相关企业应当对此予以重视。一方面，关键信息基础设施的所有或运营企业必须与政府有关部门，以及其他具有依赖性的关键信息基础设施运营者之间进行有关系统漏洞、网络入侵、攻击、预警和应对策略等关键信息基础设施网络安全相关信息的及时交换。不履行共享义务导致严重网络安全危害后果，或违反共享相关要求的应当承担法律责任。另一方面，对于企业一方在信息共享的过程中不当泄露国家机密、商业秘密，没有采取安全防护措施导致其接收的共享信息被未经授权地访问，以及并未采取技术措施移除接收的个人可识别信息导致个人隐私受到侵犯的，应当依据《国家安全法》、《保密法》、《刑法》、《民法》、《全国人大常委会关于加强网络信息保护的決定》等相关法律法规的规定承担相应的法律责任。法律责任的认定标准基于参与主体的主观目的，即政府有关部门和关键信息基础设施所有或运营企业基于主观善意实施网络安全信息共享相关法律法规授权的行为应当受到法律保护，但是，双方在网络安全信息共享的过程中基于故意或重大过失导致侵权的，应当承担相应的法律责任。

## 第四部分

### 网络产品和服务提供者 的网络安全法律遵从

第 18 章 网络产品和服务安全

第 19 章 网络安全漏洞通知和报告

第 20 章 用户信息保护

第 21 章 保密义务

第 22 章 网络关键设备和网络安全专用产品合规要求





## 第 18 章

# 网络产品和服务安全

### 第一节 《网络安全法》相关规定及释义

《网络安全法》第二十二条规定了网络产品和服务提供者的安全义务，主要包括以下几个方面。第一，应当符合相关国家标准的强制性要求。第二，网络产品、服务的提供者不得设置恶意程序。第三，安全缺陷和漏洞的告知义务：发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。第四，网络产品服务的安全维护义务：网络产品、服务的提供者应当为其产品、服务持续提供安全维护；在规定或者当事人约定的期限内，不得终止提供安全维护。

2017 年 5 月 2 日国家互联网信息办公室发布了《网络产品和服务安全审查办法》（以下简称《办法》），该办法自 2017 年 6 月 1 日起施行。《办法》规定由国家互联网信息办公室会同有关部门成立网络安全审查委员会，负责审议网络安全审查的重要政策，协调网络安全审查相关重要问题。要求对关系国家安全和公共利益的信息系统使用的重要网络产品和服务，应当经过网络安全审查。重点审查网络产品和服务的安全性、可控性。判定是否影响国家安全和公共利益，主要看产品和服务使用后，是否会危害国家政权和主权安全，是否会危害广大人民群众利益，是否会影响国家经济可持续发展及国家其他重大利益。

2017年8月30日全国信息安全标准化技术委员会发表了国家标准《信息安全技术 网络产品和服务安全通用要求（征求意见稿）》，（以下简称《要求》）。其中规定了在我国境内销售或提供的网络产品和服务必须满足的一般安全要求和增强安全要求。在我国境内销售或提供的所有网络产品和服务必须满足一般安全要求，其中网络关键设备和网络安全专用产品还必须满足增强安全要求。网络关键设备和网络安全专用产品范围，具体参照国家互联网信息办公室、工业和信息化部、公安部、国家认证认可监督管理委员会联合印发的《关于发布〈网络关键设备和网络安全专用产品目录〉的公告》。此标准适用于网络产品和服务提供者，对其所销售或提供的网络产品和服务进行安全自评估，同时也适用于第三方测评机构对在我国境内销售或提供的网络产品和服务进行安全测评。

## 第二节 网络产品和服务安全保障制度概述

网络产品和服务提供者对其所研发、生产、运维的网络产品及服务具有保障其安全性、可靠性、可控性的义务。我国《网络安全法》对网络产品和服务提供者所应满足的安全标准及后续的产品安全运维义务进行了明确规定，旨在消除或减少用户使用网络产品及服务时可能遇到的信息泄露、数据篡改、服务中断、非法远程控制等安全问题和安全风险。

### 一、相关概念释义

根据全国信息安全标准化技术委员会发表的相关国家标准文件，能够确定以下概念的具体含义和范围。首先，网络产品是指按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的硬件、软件和系统。一般意义上的网络产品包括计算机、信息终端、工控等相关设备，以及基础软件、系统软件等。

网络服务，即供方为满足需方要求提供的信息技术开发、应用活动，以及以网络技术为手段支持需方业务的一系列活动。常见的网络服务包括云计算服务、

网络通信服务、数据处理和存储服务、信息技术咨询服务、设计与开发服务、信息系统集成实施服务、信息系统运维服务等。

用户信息，即与自然人、法人或其他组织有关的信息，以及定义和描述这些信息的数据。用户信息包括个人信息，以及用户生成的文档、程序、多媒体资料，用户通信的内容、地址、时间，产品的配置、运行及位置数据，系统运行过程产生的日志等。

个人信息，即以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。

恶意程序是指那些用于实施网络攻击、干扰网络和信息系统正常使用、破坏网络和信息系统、窃取网络和系统数据等行为的程序。常见的恶意程序包括病毒、蠕虫、木马或其他影响主机、网络或系统安全、稳定运行的程序。

安全缺陷是指网络产品和服务中由于设计、开发错误、配置错误、生产问题或运维缺陷引入的可能影响网络产品和服务安全的弱点。

漏洞即脆弱性，网络产品和服务中能够被威胁利用的弱点。

## 二、网络产品和服务安全保障制度的立法背景

网络产品及服务是社会各界及普通民众进行网络活动的重要载体形式，对于其安全的保障义务则是网络产品及服务提供者最应致力履行的主要义务之一。为了能够避免产品和服务面临非法控制、干扰和中断运行的风险或产品和服务提供者利用提供产品和服务的便利条件非法收集、存储、处理、利用用户相关信息的风险，以美国为代表的许多国家建立了网络安全审查制度。在美国，外国投资委员会负责国家安全审查工作。外国投资委员会负责组织调查活动，并决定是否提请总统审议或采取一定措施；总统享有较大自由裁量权和最终决定权，当其判断交易可能危及美国国家安全时，可中断、禁止这些交易。例如，2010年5月，华为欲以200万美元收购美国服务器技术研发公司3Leaf Systems的部分资产，包括购买服务器和专利，以及聘请3Leaf Systems的15名员工，但是这一交易直到2010年11月仍未提交到美国外商投资委员会备案。2011年2月10日，5名美国国会

议员给美国财政部长盖特纳和商务部长骆家辉发邮件表示，华为这笔交易会带来国家安全风险，应当对华为收购美国的技术进行严密的审查。随后，美国海外投资委员会要求华为取消收购 3Leaf Systems 特定资产。迫于美国外商投资委员会的压力，华为最终放弃了对服务器科技公司 3Leaf Systems 特定资产的收购。

### 第三节 网络产品和服务安全保障法规遵从框架及建议

除了《网络安全法》和《信息安全技术 网络产品和服务安全通用要求》之外，我国还有其他部门法和地方规章制度对网络产品及服务的提供者应承担的安全保障义务有所规定，详情如表 18-1 所示。

表 18-1 网络产品和服务安全保障法规遵从框架

法律名称	法律条款	法律规定
《吉林省信息化促进条例》	第二十二條	从事电子信息产品制造软件开发和信息服务的企业应当按照国家标准、行业标准或者地方标准保障产品和服务质量。鼓励企业采用国际标准或者国外先进标准
《浙江省信息化促进条例》	第二十一條	从事信息技术产品制造、软件开发和信息服务的企业应当按照国家标准、地方标准和有关规范的要求，组织产品生产、技术开发和信息服务。 鼓励企业制定和实施严于国家标准、地方标准的企业产品、服务标准，提高产品和服务质量
《厦门市计算机信息系统安全保护暂行办法》	第三十一條	制造、销售、出租、维修、商业性赠送计算机产品的单位和个人，应确保其产品经检测合格，不得携带有计算机病毒和其他有害数据
《湖南省信息化条例》	第三十四條	从事信息技术产品制造、软件开发和信息服务的企业应当遵守诚实信用的原则，为用户提供优质的产品和服务。不得损害用户和其他经营者的合法权益，并按照国家标准、行业标准、地方标准和有关规范的要求，组织产品生产和技术开发
《新疆维吾尔自治区信息化促进条例》	第三十條	从事电子信息产品设计、制造、软件开发，应当按照《标准化法》的有关规定组织生产、开发，保证产品和服务质量

续表

法律名称	法律条款	法律规定
《内蒙古自治区信息化促进办法》	第二十六条	从事电子信息产品设计、制造、软件开发，应当按照《标准化法》的有关规定组织生产、开发
《计算机病毒防治管理办法》	第十四条	从事计算机设备或者媒体生产、销售、出租、维修行业的单位和个人应当对计算机设备或者媒体进行计算机病毒检测、清除工作并备有检测清除的记录
《厦门市计算机信息系统安全保护暂行办法》	第二十八条	制造、销售、出租、维修商业性赠送计算机产品的单位和个人应确保其产品经检测合格，不得携带有计算机病毒和其他有害数据
《河南省计算机信息系统安全保护暂行办法》	第十八条	任何单位和个人制造、出租、安装、维修计算机软件、硬件必须对产品进行检测，确保产品不携带有计算机病毒和其他有害数据
《深圳经济特区计算机信息系统公共安全管理规定》	第二十五条	制造、销售、出租、维修商业性赠送计算机产品的单位和个人其产品应经过检测，不得携带有计算机病毒和其他有害数据
《规范互联网信息服务市场秩序若干规定》	第七条	<p>互联网信息服务提供者不得实施下列侵犯用户合法权益的行为：</p> <p>一无正当理由拒绝拖延或者中止向用户提供互联网信息服务或者产品；</p> <p>二无正当理由限定用户使用或者不使用其指定的互联网信息服务或者产品；</p> <p>三以欺骗误导或者强迫等方式向用户提供互联网信息服务或者产品；</p> <p>四提供的互联网信息服务或者产品与其向用户所作的宣传或者承诺不符；</p> <p>五擅自改变服务协议或者业务规程降低服务质量或者加重用户责任</p>

根据我国《网络安全法》的第二十二条明确规定，网络产品、服务提供者所提供网络产品及服务应符合相关国家标准强制性要求，并且不得在其中设置恶意程序，应当持续为用户提供应有的安全运维服务。随后国家互联网信息办公室发布的《网络产品和服务安全审查办法》（以下简称《办法》）及全国信息安全标准化技术委员会发表的国家标准《信息安全技术 网络产品和服务安全通用要求（征求意见稿）》（以下简称《要求》）也对这些义务进行了详细的说明和规定。

网络产品和服务安全保障制度遵从建议如表 18-2 所示。

表 18-2 网络产品和服务安全保障制度遵从建议

控制项	网络产品和服务安全保障制度的法规遵从建议	对应条款
恶意程序防范	网络产品和服务提供者在提供产品和服务的过程中应杜绝以下禁止项： （1）禁止在网络产品和服务的研发、生产、交付、运维等过程中植入恶意程序； （2）禁止在网络产品和服务中设置隐蔽接口或未明示功能模块，如隐蔽的管理接口或调试接口； （3）禁止加载能够禁用或绕过安全机制的组件，不存在硬编码方式的默认口令和隐藏账号； 网络产品和服务提供者在提供产品和服务的过程中应履行以下义务： （1）建立和实施网络产品和服务的完整性保护措施，减少产品和服务的关键组件、过程和数据被篡改、伪造的风险； （2）保护用户对软件安装、使用、升级、卸载的知情权和选择权，安装和升级软件时必须明示告知用户并获得用户同意，允许用户卸载产品核心功能之外的软件，禁止通过技术手段强制或诱导用户安装和升级用户不知情的软件； （3）通过用户协议、产品使用说明书、门户网站等途径，承诺提供的网络产品和服务不包含恶意程序、隐蔽接口或未明示功能模块等	第二十二条 网络产品、服务应当符合相关国家标准的强制性要求。网络产品、服务的提供者不得设置恶意程序；发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。
	网络产品和服务提供者在提供产品和服务的过程中应履行以下义务： （1）在国家法律、行政法规、部门规章等规范性文件规定或与用户约定的期限内，为网络产品和服务提供持续的安全维护； （2）在国家法律、行政法规、部门规章等规范性文件规定或与用户约定的期限内，不因业务变更、产权变更等原因单方面中断或终止安全维护	网络产品、服务的提供者应当为其产品、服务持续提供安全维护；在规定或者当事人约定的期限内，不得终止提供安全维护

第四节 监督管理与法律责任

《网络安全法》第六十条明确规定，违反本法第二十二条第一款、第二款和第四十八条第一款规定，在其提供的网络产品或服务中设置恶意程序的；或对其产品、服务存在的安全缺陷、漏洞等风险未立即采取补救措施，或者未按照规定及时告知用户并向有关主管部门报告的或擅自终止为其产品、服务提供安全维护的网络产品或者服务的提供者，由有关主管部门责令改正，给予警告；被责令改正、

警告之后拒不改正或者直接导致危害网络安全等后果的，处五万元以上五十万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款：

《网络安全法》第二十三条还规定了网络关键设备和网络安全专用产品应当按照相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求后，方可销售或者提供。国家网信部门会同国务院有关部门制定、公布网络关键设备和网络安全专用产品目录，并推动安全认证和安全检测结果互认，避免重复认证、检测。

# 网络安全漏洞通知和报告

## 第一节 《网络安全法》相关规定及释义

随着信息化的普及和软硬件的广泛应用，由于技术不成熟或人为因素造成的漏洞利用问题也日渐凸显，作为重要的安全风险之一，漏洞的法律治理引起了社会各界越加广泛的关注，安全漏洞的风险告知义务逐渐演变为网络产品和服务提供者的重要义务。2016 年 11 月发布，2017 年 6 月已经全面实施的《网络安全法》以基本法的地位规定了漏洞的告知义务，虽然只有简短的一款，但是我国首次在立法中予以确认，分析条款可知，该款不仅将漏洞定性为安全风险，还规定了网络产品和服务提供者要将其告知用户和有关主管部门。

《网络安全法》第二十二条第一款规定，网络产品、服务的提供者发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。该条款规定了网络产品和服务安全漏洞的通知和报告义务，该义务的遵从主体为网络产品和服务的提供者，义务内容为当网络产品和服务的提供者发现其提供的网络产品和服务存在安全缺陷、漏洞等风险时，应该立即采取补救措施，同时，按照规定及时告知用户，并报告给有关主管部门。与此项义务相对应的权利主体是用户及有关主管部门。一方面，该条款主要保护的是用户的知情权，提前告知风险目的在于提前准备，预防安全事件的发生；另



一方面,告知有关主管部门是落实网络安全监测预警与信息通报制度的具体要求。

## 第二节 网络安全漏洞通知和报告制度概述

### 一、网络安全漏洞通知和报告制度的立法背景

鉴于信息化时代的迅速发展,我国网络利用率迅速普及,据第 40 次《中国互联网络发展状况统计报告》显示,截至 2017 年 6 月,我国网民数规模达到 7.51 亿,占全球网民总数的 1/5,互联网普及率为 54.3%,超过全球平均水平 4.6 个百分点<sup>①</sup>。安全漏洞是信息技术发展现阶段不可避免的,且会长期普遍存在,被黑客利用进行攻击的事件层出不穷,且危害范围逐渐扩大。从“熊猫烧香”到“震网”、“火焰病毒”、“心脏滴血”等事件,从全球最大的社交网站 Facebook 遭攻击,个人数据泄露,到索尼游戏平台被犯罪分子发现漏洞进行破坏。利用软件漏洞对关键基础设施领域的攻击层出不穷,几乎每个国家,各个企业都遭遇过不同程度的数据窃密、系统破坏。在我国网民大规模增长的全球信息化时代,恐怖分子利用漏洞进行攻击的范围越来越广,从窃取用户个人隐私数据,未经授权访问银行、金融、交通、教育等各大行业,到攻入政府、国家网站进行数据篡改、毁坏,影响国家安全及政治稳定。

2012 年 11 月,因为巴勒斯坦和以色列的领土冲突问题,致使黑客不断对以色列总统、政府网站、国防部计算机系统进行攻击。2013 年 1 月 16 日,墨西哥反政府组织中一名自称“墨西哥匿名者”的黑客组织利用软件漏洞对国防部网站攻击,并贴上煽动国家分裂的宣言,导致两小时的服务中断,并且该组织在社交网站上示威性的炫耀已经成功破坏了国防部网站。2014 年 4 月被首次曝光的“心脏滴血”漏洞,在当时引起了轩然大波,因为黑客可以通过它向全球 2/3 的网络服务器发动攻击。2015 年,因网站存在高危漏洞导致我国 2 000 万条开放数据泄露。2016 年 10 月,攻击者利用中心路由器“Vaccine Routing Server”上存在的安

<sup>①</sup> 参考 <http://news.china.com/news100/11038989/20170804/31039433.html>。

全漏洞，攻击了韩国军事网络指挥中心。2017 年 4 月，由于电脑黑客入侵，美国得克萨斯州达拉斯所有紧急警报系统在夜里鸣叫了 90 分钟左右，这是至今出现的最大规模警报系统入侵事故。

据国家信息安全漏洞库统计，2017 年 7 月采集安全漏洞共 1 190 个，Apple iOS 系统成为黑客重要攻击目标；7 月国家信息安全漏洞库接报漏洞共计 2 159 个，其中信息技术产品漏洞（通用型漏洞）68 个，网络信息系统漏洞（事件型漏洞）2 090 个。仅仅一个月时间，被发现的安全漏洞数量超过 3 000 个，且几个月的平均数量均是如此，可见安全漏洞的广泛性。任何网络产品在目前技术水平阶段几乎都存在已知或未知的网络安全漏洞，且随时有被利用的风险。存在风险及时告知用户，使用户更加容易理解和掌握风险信息从而进行有的放矢的行动，还可以减少用户与企业之间不必要的误会与隔阂，报告相关主管部门则可以协同各方力量一起研究补丁，及早进行修复。

## 二、网络安全漏洞通知和报告制度的必要性

维护网络空间安全是一项重大的战略挑战，这需要全社会的共同努力。网络产品和服务提供者作为通过计算机网络向消费者提供服务的机构和组织，被认为是有效预防和解决网络安全问题的核心因素，网络产品和服务提供者的责任和义务成为保障网络安全的重要环节。在提供的网络产品和服务中，用户的知情权不仅应当包括传统意义上的对经营者自身及其提供商品或者服务的情况的知悉，更应当包括对网络产品和服务提供者的网络安全状况，特别是对存在的网络安全漏洞风险。因为网络产品和服务提供者的计算机网络安全状况不仅直接关系到服务和交易的顺利进行，而且网络产品和服务提供者在提供服务的同时往往会掌握用户的个人敏感信息，一旦其网络出现漏洞，发生危险，就可能使用户的个人信息受到非法窃取和盗用，损害其人身和财产利益。因此，网络产品和服务提供者发现自己的计算机网络存在安全漏洞和其他风险时，应该及时向其消费者和用户进行告知，并采取适当的措施，避免发生损害用户利益的安全事件或尽量减少损害。这不仅是消费者知情权的体现，也是保障消费者安全权的要求。另外，网络安全漏洞报告制度也是落实网络安全信息通报制度的具体要求，向有关主管部门报告

能够在行业内部提前报告风险发生的可能性,协同社会各方主体参与漏洞的修复,降低漏洞被利用的概率。

### 三、网络安全漏洞通知和报告制度的相关概念释义

漏洞 (Vulnerability), 又称脆弱性, 这一概念的出现已有 30 多年历史, 技术、学术和产业界从不同角度给出了不同的定义。目前普遍接受的定义是: 漏洞是一个或多个威胁可以利用的一个或一组资产的弱点, 是违反某些环境中安全功能要求的评估对象中的弱点, 是在信息系统 (包括其安全控制) 或其环境的设计及实施中的缺陷、弱点或特性。这些缺陷或弱点可被外部安全威胁利用。漏洞是“非故意”产生的缺陷, 具备能被利用而导致安全损害的特性。网络安全漏洞具备可利用性、难以避免性、普遍性和长存性等技术特征。为强调漏洞可能导致的网络安全风险, 各界基本将漏洞和网络安全漏洞的概念混用不加区分, 漏洞称之为内在的脆弱性, 与之相对的是外部安全威胁, 内部脆弱性和外部安全威胁结合起来共同构成安全风险。

针对网络安全漏洞本身, 尽管国内外立法缺少明确的概念界定, 但均延续了传统信息安全的内外两分法, 将网络安全漏洞纳入安全风险和网络安全信息范畴予以规制。在安全风险层面, 《网络安全法》第二十五条规定将系统漏洞 (内部脆弱性) 和计算机病毒、网络攻击、网络侵入等外部安全威胁作为整体安全风险, 强调了网络运营者的风险控制和应急处置责任。美国 2015 年《网络安全信息共享法》(Cybersecurity Information Sharing Act of 2015, CISA) 强调网络安全的目的是“保护信息系统或者使在信息系统存储、处理、传输的信息免于网络安全威胁或网络安全漏洞的侵害”, 也将网络安全威胁和网络安全漏洞并列, 作为安全风险予以共同防范和控制。相比之下, 《关键信息基础设施安全保护条例 (征求意见稿)》第三十五条规定将漏洞纳入“安全威胁信息”范畴, 则存在定义使用上缩小化的误区。在网络安全信息层面, 《网络安全法》第二十六条通过列举方式界定了网络安全信息的一般范围, 包括系统漏洞、计算机病毒、网络攻击、网络侵入等, 将漏洞作为第一位的网络安全信息, 也体现了网络安全信息承载网络安全风险的基本功能。

《网络安全法》第二十二条第一款中的“风险”在这里意指网络环境中可能发

生安全事件的概率。《信息技术—安全技术—信息安全风险管理》(ISO27005)对信息安全风险进行了解释,“某种特定的威胁利用资产或一组资产的脆弱点,导致这些资产受损或破坏的潜在可能”。《信息技术安全技术—信息安全管理实用规则》(ISO27002)规定:风险指事件的概率及其结果的组合。由此可见,风险是计算机信息系统或者网络产品、服务中常见的,以现在的技术水平难以避免,需要安全研究人员及时采取补救措施,预防或降低损害的一个或一组弱点。

## 四、网络安全漏洞通知和报告的方式及其内容

根据我国实践和美国《加州披露法》(The California Disclosure Law)的规定,网络产品和服务提供者的安全漏洞告知方式包括:①口头形式(主要是通过电话方式,由于这种方式成本较高,需耗费大量人力和时间,所以使用较少)、短信形式、书面形式(写在纸上并邮寄);②电子形式(如电子邮件,但是必须是服务使用者事先表示同意接受这种形式并符合联邦《电子签名法》的规定);③弹框形式(弹框告知使用较多,且在弹框告知之际,一般已经有研发好的补丁可以修复漏洞,这种方式是目前常用的方式之一)。比较而言,邮件告知的成本较小,加上信息系统的无国界性,经过邮件加密发送也可以减小信息泄露的概率,美国国家基础设施委员会 2004 年向总统提交的漏洞披露政策将漏洞信息规定为敏感机密的信息,要求对漏洞沟通的所有电子邮件都必须进行加密,这必然包括通过邮件向用户告知或是向主管机关报告漏洞信息。

此外,鉴于安全漏洞的特殊性及近些年资源属性迅速凸显,漏洞信息本身的价值更为复杂,向用户告知的内容和向有关主管部门报告的内容也应慎重考虑。首先,毋庸置疑的,应向用户和有关主管部门说明某个产品或服务存在安全漏洞这一事实。其次,关于漏洞的详细信息方面,对于用户和主管部门应该有所区分。对用户而言,只要知道漏洞存在,加以防范即可,因此为避免漏洞详细信息被恶意利用,只需告知用户存在什么性质的漏洞即可(如漏洞的类型)。主管机关与用户不同,主管机关担负着监督漏洞修补、调动各方力量共同研究补丁的职责,因此在向主管机关报告安全漏洞时,不仅应报告漏洞的基本信息,还应报告漏洞的详细信息,这样有利于主管机关发挥监管职责,共享漏洞并协调各方力量尽快修

复。再次，应该告知安全漏洞可能造成的后果及用户可以采取的降低风险的措施。最后，在补丁修复或者找到其他解决办法之后，也应及时向用户告知。

### 第三节 网络安全漏洞通知和报告

#### 法规遵从框架及建议

告知用户安全漏洞意味网络产品和服务提供者承认其自身产品和服务的缺陷，对其是一个巨大挑战，实际操作层面也存在障碍，过去立法中几乎没有涉及相关条款。少有的可适用的规定主要体现在《消费者权益保护法》中，其第十九条规定：经营者发现其提供的商品或者服务存在缺陷，有危及人身、财产安全危险的，应当立即向有关行政部门报告和告知消费者，并采取停止销售、警示、召回、无害化处理、销毁、停止生产或者服务等措施。采取召回措施的，经营者应当承担消费者因商品被召回支出的必要费用。虽然该条规定与《网络安全法》的内容在义务主体、发生条件、采取措施有所差异，单本质上都是为了保护消费者或用户的合法权益，规范市场秩序。相比而言，《网络安全法》更加强调网络环境中发生的网络产品的质量缺陷，注重规范最近几年新出现的漏洞等新型安全风险。鉴于网络产品和服务的特殊性，一旦使用难以召回，因此《网络安全法》规定的更为宏观，以“立即采取补救措施”概括规定，而《消费者权益保护法》则采用列举加概括的方式，先列举了停止销售、警示、召回、无害化处理、销毁、停止生产或者服务的具体措施，又以“等措施”加以概括，这也是顺应时代发展，更好的适用信息化社会发展需求的立法变革。

网络安全漏洞通知和报告法规遵从框架如表 19-1 所示。

表 19-1 网络安全漏洞通知和报告法规遵从框架

法律名称	法律条款	法律规定
《网络安全法》	第二十二条	网络产品、服务应当符合相关国家标准的强制性要求。网络产品、服务的提供者不得设置恶意程序；发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告

续表

法律名称	法律条款	法律规定
《消费者权益保护法》	第十九条	经营者发现其提供的商品或者服务存在缺陷，有危及人身、财产安全危险的，应当立即向有关行政部门报告和告知消费者，并采取停止销售、警示、召回、无害化处理、销毁、停止生产或者服务等措施。采取召回措施的，经营者应当承担消费者因商品被召回支出的必要费用
《关键信息基础设施安全保护条例（征求意见稿）》	第三十三条	运营者发现使用的网络产品、服务存在安全缺陷、漏洞等风险的，应当及时采取措施消除风险隐患，涉及重大风险的应当按规定向有关部门报告
《互联网网络安全信息通报实施办法》	附件一 信息报送项目 (一) 基础电信业务经营者	本单位网内漏洞等网络安全隐患及处置情况
	附件一 信息报送项目 (二) 互联网域名注册管理、服务机构	域名系统相关的系统漏洞等网络安全风险信息及处置情况
《工业控制系统信息安全防护指南》	第二条	密切关注重大工控安全漏洞及其补丁发布，及时采取补丁升级措施。在补丁安装前，需对补丁进行严格的安全评估和测试验证
《公共互联网网络安全威胁监测与处置办法》	第二条	本办法所称公共互联网网络安全威胁是指公共互联网上存在或传播的、可能或已经对公众造成危害的网络资源、恶意程序、安全隐患或安全事件，包括：(三) 网络服务和产品中存在的安全隐患，包括硬件漏洞、代码漏洞、业务逻辑漏洞、弱口令、后门等

《信息技术 安全技术 信息安全管理实用规则》(ISO27002) 第 13 节专门规定了信息安全事故管理，其中 13.1 指出，报告信息安全事件和弱点所要实现的目标是“确保与信息系统有关的信息安全事件和弱点能够以某种方式传达，以便及时采取纠正措施”。为了实现该目标，“应有正式的事件报告和上报程序。所有雇员、承包方人员和第三方人员都应了解用来报告可能对组织的资产安全造成影响的不同类型的事件和弱点的程序。应要求他们尽可能快地将信息安全事件和弱点报告给指定的联系点”。13.1.2 具体指出了报告安全弱点的控制措施和实施指南，控制措施是“应要求信息系统和服务的所有雇员、承包方人员和第三方人员记录

并报告他们观察到的或怀疑的任何系统或服务的安全弱点”。在实施层面规定：为了预防信息安全事故，所有雇员、承包方人员和第三方人员应尽可能快地将这些事情报告给他们的管理者，或者直接报告给服务供应商。报告机制应尽可能容易、易理解和方便可用。应告知他们，在任何情况下，他们都不应试图去证明被怀疑的弱点。

ISO27002 规定的弱点即为安全风险，包括网络安全漏洞，该标准比《网络安全法》规定的更为详细，义务主体更为宽泛，不仅包括网络产品和服务提供者，也包括所有雇员、承包方人员和第三方人员，但这些人员报告的对象不是用户和主管机关，而是其管理者或服务供应商。这实际是限制了安全漏洞被不负责任披露的可能性，漏洞本身的复杂性决定了其告知之后可能发生的安全事件危害要远远大于其他弱点和缺陷，因此将告知限定在网络产品和服务提供者这一单一主体是有必要的，可以减少公开披露漏洞被黑客利用的风险。

网络安全漏洞通知和报告法规遵从建议如表 19-2 所示。

表 19-2 网络安全漏洞通知和报告法规遵从建议

控制项	网络安全漏洞通知和报告法规遵从建议	对应条款
1. 网络安全漏洞的通知和报告		第二十二 条第一款 网络产品、服务应当符合相关国家标准 的强制性要求。网络产品、服务的提供者不得设置恶意程序；发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告
缺陷漏洞管理	网络产品和服务提供者应当在发现网络产品和服务存在安全缺陷、漏洞时，立即采取修复或替代方案等补救措施，按照国家网络安全监测预警和信息通报制度等规定，及时告知用户安全风险，并向有关主管部门报告	
2. 网络安全漏洞管理的原则		
公平、公开、公正原则	厂商在处理自身产品的漏洞时应坚持公开、公正原则。漏洞管理组织在处理漏洞信息时应遵循公平、公开、公正原则	
及时处理原则	用户、厂商和漏洞管理组织在处理漏洞信息时都应遵循及时处理的原则，及时消除漏洞与隐患	
安全风险最小化原则	在处理漏洞信息时应以用户的风险最小化为原则，保障广大用户的利益	
通报形式	通过统计分析图形、报表方式展示； 通过关键字快速检索获取相关日志和流量元数据及详细信息，查询追溯事件的相关原始信息； 通过展示攻击过程和扩散路径，进行攻击链和攻击上下文信息的呈现，多维度展示安全威胁的影响和范围	
3. 网络安全漏洞管理的规划		

续表

控制项	网络安全漏洞通知和报告的法规遵从建议	对应条款
	<p>根据漏洞生命周期中漏洞所处的不同状态，将漏洞管理行为对应为预防、收集、消减和发布等实施活动。</p> <p>预防是指通过各种安全手段提高信息系统的安全水平，避免漏洞的产生和恶意利用。</p> <p>收集是针对已发现的漏洞进行信息的及时跟踪与获取。</p> <p>消减是指在漏洞被发现后积极采取补救措施，最大限度减少漏洞带来的损失。</p> <p>发布是指在遵循一定的发布策略的前提下，对漏洞及其修复信息进行发布。</p> <p>用户、厂商和漏洞管理组织应依据本标准建立符合自身特点的漏洞处理策略和处理流程</p>	
4. 网络安全漏洞管理的实施		
漏洞的预防	厂商应尽可能地采用安全开发生命周期，在需求、设计、实现、配置、运行等阶段采取风险分析、代码审查、渗透测试等手段，提高产品安全性	
漏洞的收集	<p>厂商应提供接收漏洞信息的渠道，如网站、邮件或电话等。</p> <p>厂商应对漏洞发现者或漏洞管理组织报告的漏洞在规定时间内确认其是否真实存在，并回复报告方</p>	
漏洞的消减	<p>厂商应遵循及时处理原则，依据厂商对漏洞的消减处理策略，对发现的漏洞在规定时间内进行修复，依据 GB/T AAAAA-20XX 确定漏洞的危害等级，优先开发高危漏洞的修复措施。</p> <p>厂商应保证补丁的有效性和安全性，并进行兼容性测试，避免因更新补丁而对产品或系统带来影响或新的安全风险。</p> <p>厂商应为发现的漏洞开发解决方案。解决方案的开发过程包含更加细致的调查过程，包括调查漏洞更深层的原因，以及确定其他产品是否有同样或者类似的漏洞。厂商最终需开发出补丁或者临时修复措施，同时测试检验修复措施的有效性、安全性和兼容性，不能破坏原系统的功能。厂商在发布漏洞信息和修复措施后，关注用户反馈，考虑是否需对漏洞修复进一步完善</p>	
漏洞的发布	厂商应建立发布渠道，在规定时间内发布漏洞信息及修复措施，并通知用户	
5. 网络安全漏洞的处理策略		



续表

控制项	网络安全漏洞通知和报告的法规遵从建议	对应条款
漏洞处理时间	在不同的漏洞管理活动中对漏洞进行处理时所规定的时间不同，相关人员或组织必须在规定时间内完成对漏洞的处理。 具体而言，对漏洞的验证不超过 10 个工作日，对漏洞的反馈不超过 5 个工作日，针对漏洞开发修复措施的时间不超过 30 个工作日，通报漏洞管理组织的时间不超过 5 个工作日，发布漏洞信息及修复措施的时间不超过 5 个工作日	
漏洞管理组织关于漏洞通报的处理策略	漏洞管理组织在对漏洞进行验证之后，应对受影响产品的厂商进行通报，敦促其及时开发修复补丁。厂商应在接到通知后 5 个工作日内给予正式反馈，并给出漏洞修复时间表，如逾期不予反馈，或无法与厂商取得联系，则漏洞管理组织有权对漏洞内容进行公布，以提示用户修复，因漏洞公布给用户带来的损失，由厂商承担	
漏洞管理组织关于厂商修复漏洞的处理策略	厂商应在确认漏洞信息后 30 个工作日内提供补丁或修复措施；由于技术或其他不可抗拒的原因导致 30 个工作日内无法完成补丁开发，可根据厂商申请情况酌情延长漏洞修复时间。否则漏洞管理组织有权对漏洞内容进行公布，以提示用户修复，因漏洞公布给用户带来的损失，由厂商承担。漏洞管理组织可以联系信息安全厂商或其他安全机构针对该漏洞给出修复措施	

第四节 监督管理与法律责任

《网络安全法》第八条规定，国家网信部门负责统筹协调网络安全工作和相关监督管理工作。国务院电信主管部门、公安部门和其他有关机关依照本法和有关法律、行政法规的规定，在各自职责范围内负责网络安全保护和监督管理工作。县级以上地方人民政府有关部门的网络安全保护和监督管理职责，按照国家有关规定确定。本条对于网络安全漏洞通知和报告的监督管理机构做出了规定，即国家网信部门负责统筹协调网络安全漏洞通知和报告的具体工作，国务院电信主管部门、公安部门和其他有关机关依照本法和有关法律、行政法规的规定，在各自职责范围内负责网络安全漏洞通知和报告的监督管理工作。县级以上地方人民政

府有关部门按照国家有关规定负责具体实施本行政区域内的网络安全漏洞通知和报告的监督管理工作。

《消费者权益保护法》第十九条只规定了相关主体的风险告知义务，没有规定具体的处罚措施。《网络安全法》是一部以预防、治理、惩罚为一体的综合性保障法，不仅提出了网络安全漏洞的通知和报告义务，还规定了违反该义务的处罚措施，其第二十二条构成了对《消费者权益保护法》的有效衔接。根据《网络安全法》第六十条规定，违反第二十二条第一款规定的网络安全漏洞通知和报告义务，对其产品、服务存在的安全缺陷、漏洞等风险未立即采取补救措施，或者未按照规定及时告知用户并向有关主管部门报告的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处五万元以上五十万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。如果存在安全漏洞而不立即采取补救措施、未按照规定及时告知用户、未向有关主管部门报告，只要违反其中一种行为，轻则被责令改正、给予警告；拒不改正或者发生危害网络安全等后果的，要处罚网络产品和服务提供者及直接负责的主管人员，可见《网络安全法》规定的处罚措施比较具体且严重，网络产品和服务提供者应谨遵法律规定，切实履行网络安全漏洞的风险告知义务。

## 第 20 章

# 用户信息保护

随着信息技术广泛应用和大数据业务的兴起，通过对用户信息的收集和使用，可以使得网络产品和服务的提供者对其服务的用户进行精准画像，分析并预先掌握用户潜在的服务需求，从而帮助网络产品和服务提供者更为有效的优化用户体验、提升其网络产品和服务的质量、增加用户黏性并提高其在同行业内的竞争力。因而，对于网络产品和服务提供者而言，其拥有的用户信息数据越多，其在业务运营中的竞争优势就越大，因而用户信息数据作为各个网络产品和服务提供者业务经营的核心竞争力之一，成为网络产品和服务提供者在业务运营中所不肯错过的优势运营资源。

然而，机遇永远伴随着挑战，网络安全形式日益严峻，网络渗透、网络攻击、网络恐怖和违法犯罪等无不严重危害着用户信息安全，严重损害国家、企业和个人利益，影响社会和谐稳定<sup>①</sup>。因而，对于用户信息安全的保护一直是网络产品和服务提供者在网络安全法律遵从工作中的重中之重，也一直是各国的监管重点。

### 第一节 《网络安全法》相关规定及释义

《网络安全法》第二十二条明确规定：网络产品、服务具有收集用户信息功能

<sup>①</sup> 参考国家互联网信息办公室《国家网络空间安全战略》。

的，其提供者应当向用户明示并取得同意；涉及用户个人信息的，还应当遵守本法和有关法律、行政法规关于个人信息保护的规定。

实践中，网络产品和服务所服务的用户可能是自然人，也可能是政府部门或企业等，因此其所收集的用户信息除用户个人信息<sup>①</sup>外，可能也涉及一些商业秘密信息、国家安全信息等。此外，即使仅针对自然人用户，网络产品和服务所收集的用户信息，除了用户个人信息之外，也还会涉及一些不含有用户个人信息的信息数据，如用户的通信内容、用户的社交关系、健康状况、用户使用习惯及其他在使用网络产品和服务中所提交或形成的信息数据。

因此，对于用户信息的保护应该至少包含如下两部分：①对于含有用户个人信息的用户信息的保护；②对于不含有用户个人信息的其他用户信息的保护。

## 第二节 网络产品和服务的用户信息保护制度概述

目前，国际上对于用户信息的保护规定，主要集中于对于用户个人信息和用户个人隐私的保护，如欧盟于2016年4月14日投票通过“史上最严格的数据保护条例”《一般数据保护条例》，严格规定了对个人信息保护、监管、处罚措施，以此实现对于用户个人数据的保护；美国通过《消费者隐私权利法案》、《儿童在线隐私权保护法案》等，澳大利亚通过《隐私权法》等，从对个人隐私权保护的角度实现对于用户个人信息的保护。但对于不包含个人信息的用户信息保护却鲜有规定。

因此本章节主要基于我国现行有效的相关法律、行政法规规定和相关法律法规已公开发布的征求意见稿，及有关国家标准、行业标准（及其草案）梳理形成。

---

①《网络安全法》第七十六条第五款：个人信息，是指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。

## 一、用户信息保护的基本原则

### （一）明示原则及用户同意原则

对于用户信息的收集，首先应遵从明示原则，明确向用户告知、说明、警示对于所有用户信息的收集/使用的目的、方式和范围，以及有关用户信息安全保护的措施等信息。如果网络产品和服务的提供者是通过格式合同（如用户服务协议、隐私政策等）方式与用户达成用户信息保护条款的，还应注意采用显著方式提请用户注意有关用户信息保护的与其有重大利害关系的、对其权利可能造成影响的条款，例如网络产品和服务的提供者的免责条款，网络产品和服务的提供者与第三方之间有关用户信息的共享使用等。其次，对于用户信息的收集和使用等还应遵从用户同意原则，即仅在用户明确同意的范围内对用户信息进行收集、使用。网络产品和服务提供者在运营过程中若对用户信息的收集和使用规则进行修改的，则针对修改过的相关规则仍应重新取得用户的同意。

### （二）合法、正当、必要原则

我国多部现行法律法规规定了对个人信息收集、使用的合法、正当、必要原则，如《网络安全法》第四十一条规定：网络运营者<sup>①</sup>收集、使用个人信息，应当遵循合法、正当、必要的原则……；《关于加强网络信息保护的决定》明确规定：网络服务提供者和其他企业事业单位在业务活动中收集、使用公民个人电子信息，应当遵循合法、正当、必要的原则……；《电信和互联网用户个人信息保护规定》第五条规定：电信业务经营者、互联网信息服务提供者在提供服务的过程中收集、使用用户个人信息，应当遵循合法、正当、必要的原则；《网络交易管理办法》第十八条规定：网络商品经营者、有关服务经营者在经营活动中收集、使用消费者或者经营者信息，应当遵循合法、正当、必要的原则……。其虽主要是针对用户个人信息收集、使用的原则。但鉴于网络产品和

---

<sup>①</sup> 根据我国《网络安全法》的第七十六条第三款的规定，网络运营者，是指网络的所有者、管理者和网络服务提供者。因此，《网络安全法》中有关网络运营者的规定也适用于网络产品和服务的提供者。

服务用户的广泛性，其在用户信息收集使用过程中极可能涉及含有个人隐私、商业秘密乃至国家秘密等敏感信息的用户信息数据，因此对于不含有个人信息的用户信息的收集和使用也应遵从合法、正当、必要的原则。网络产品和服务提供者对于用户信息的收集和使用应符合相关法律、行政法规的规定或网络产品和服务提供者与用户达成的约定，其所收集的用户信息应为实现网络产品和服务功能所必需的并仅用于正当商业目的，不得将用户信息用于提供服务之外的目的。

（三）其他原则

此外，网络产品和服务提供者对于用户信息保护义务的履行，除应注意遵从有关法律、行政法规的规定之外，还应注意遵从网络产品和服务在生产运营过程中涉及的有关国家标准和行业标准的要求。当前我国虽暂未正式发布针对不含个人信息的其他用户信息的有关国家标准，但全国信息安全标准化技术委员会于 2017 年年初发布的《信息安全技术大数据安全管理指南（草案）》（以下简称《管理指南草案》）中明确提出了有关数据收集、数据存储、数据使用、数据分发、数据删除等主要阶段的大数据安全管理基本概念和管理要求，且《管理指南草案》适用于所有的组织，包括企业、政府部门、非营利机构等。换言之，《管理指南草案》适用于网络产品和服务的提供者。因此，虽然《管理指南草案》仅为国家推荐标准，但其对于网络产品和服务提供者遵从用户信息保护义务，也具有十分重要的参考意义。根据《管理指南草案》的规定，数据安全原则主要有八项，具体如表 20-1 所示。

表 20-1 《管理指南草案》数据安全原则

原则 1 职责明确原则	根据数据规模、数据重要性、组织规模等因素，组织 <sup>①</sup> 可成立安全管理团队 <sup>②</sup> ； 组织应明确组织内部不同角色的数据安全职责； 组织应明确大数据生命周期各活动的实施主体及安全责任
-------------	---

① 《信息安全技术大数据安全管理指南（草案）》：3.1.3 组织，由作用不同的个体为实施共同的业务目标而建立的机构。组织可以是一个企业、事业单位、政府部门等。

② 《信息安全技术大数据安全管理指南（草案）》：7.2 数据安全团队的具体职责有 a) 应确定各种数据的分类分级初始值，制定数据分类分级指南；b) 应综合考虑相关的法律法规、政策、标准、大数据分析技术当前水平、组织所处行业特殊性等，综合评估数据安全分析，制定数据安全的基本要求；c) 建立相应的数据安全监督机制，监视数据安全机制的有效性；d) 负责组织的大数据安全过程，并对外部相关方（如国家安全的主管部门、数据主体等）负责；e) 对于组织的数据使用，大数据安全管理团队具有相应的权力、职责和管理责任。

续表

原则 2 意图合规原则	<p>对数据的收集、使用需局域法律依据。组织应制定相关流程确保数据的收集和使用方式没有违反任何法律义务，包括法律法规、合同条款等。组织需要确保履行承担的内部和外部的责任，包括但不限于：</p> <p>确保所有数据集和数据流的安全；</p> <p>正确处理个人信息、重要信息；</p> <p>实施了合理的跨组织数据保留的策略和实践；</p> <p>理解数据相关的法律义务，并确保组织履行了这些义务</p>
原则 3 质量保障原则	<p>组织应实施适当的措施确保数据的准确性、相关性、完整性和时效性；</p> <p>建立控制机制定期检查收集和存储的数据的质量</p>
原则 4 数据最小化原则	<p>组织应采取适当的措施最小化大数据生命周期各活动涉及的数据</p>
原则 5 责任不随数据转移原则	<p>当前控制数据的组织应对数据负责，当数据转移给其他组织时，责任不随数据转移而转移；</p> <p>组织在数据转移前，需对数据进行风险评估，确保数据转移后的风险可承受，方可转移数据。对数据转移给其他组织所造成的数据安全事件承担责任；</p> <p>组织在数据转移前，需确保通过合同或其他注入强制的内部策略等明确界定了接收方接收的数据范围和要求，确保其提供同等或更高的数据保护水平</p>
原则 6 最小授权原则	<p>在保证组织业务功能完整实现的基础上应赋予数据活动中的各角色最小的操作权限，确保非法用户或异常操作所造成的损失最小；</p> <p>所有角色只能使用所授权范围内的数据，非授权范围内的数据使用必须进行授权审批</p>
原则 7 数据保护原则	<p>组织需对数据进行分类分级，对不同安全级别的数据实施恰当的安全保护措施；</p> <p>组织应确保处理大数据平台及应用的安全控制措施和策略有效，保护数据的完整性、保密性和可用性，确保数据在整个生命周期里，免遭如未经授权访问、破坏、篡改、泄露或丢失等风险；</p> <p>组织应解决风险评估和安全检查中所发现的风险和脆弱性，并对数据安全保护措施不当所造成的安全事件承担责任</p>
原则 8 可审计原则	<p>对数据进行修改、查询、导出、删除等操作时，组织需要记录相应的操作，记录应可追溯可审查</p>

二、用户信息处理生命周期的制度要求

《网络安全法》规定“国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：①制定内部安全

管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；②采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施；③采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；④采取数据分类、重要数据备份和加密等措施；⑤法律、行政法规规定的其他义务”。若网络运营者不履行前述网络安全保护义务的，“由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处一万元以上十万元以下罚款，对直接负责的主管人员处五千元以上五万元以下罚款”。若网络产品和服务提供者不履行法律、行政法规规定的信息网络安全管理义务，经监管部门责令采取改正措施而拒不改正，致使用户信息泄露，造成严重后果的，则依据《刑法》的规定，构成拒不履行信息网络安全管理义务罪，将被判处三年以下有期徒刑、拘役或者管制，并处或者单处罚金。

对于网络产品和服务的提供者而言，其安全保护义务应贯穿于用户信息处理的所有环节中。具体而言，用户信息处理的主要环节可具体分为收集、传输存储、使用、转移/共享和删除等。

## （一）用户信息的收集

实践中，网络产品和服务收集用户信息的渠道主要可以分为如下几种。

### 1. 直接从用户处获取用户信息

网络产品和服务提供者直接从用户处获取用户信息具体又可以细分为用户上传的用户信息及用户在使用网络产品和服务中生成并同意网络产品和服务系统自动收集的用户信息。

对于直接从用户处获取的用户信息，网络产品和服务提供者应遵从我国现行有关法律规定，向用户明示用户信息收集、使用的目的、方式和范围，给予用户充分的知情权和选择权<sup>①</sup>，在明确取得用户的授权后方可遵从合法、正当、必要的原则在用户授权范围内对该等用户信息进行收集和使用。若用户上传的用户信息中含有第三方的用户信息时，网络产品和服务提供者还应注意履行诚信善意

---

<sup>①</sup> 例如，中共中央办公厅、国务院办公厅印发的《关于促进移动互联网健康有序发展的意见》中明确提出，维护用户合法权益。完善移动互联网用户信息保护制度，严格规范收集使用用户身份、地理位置、联系方式、通信内容、消费记录等个人信息行为，保障用户知情权、选择权和隐私权。



的注意义务并采取必要的管理审核措施，以确保该等归属于第三方的用户信息也已取得充分合法的授权可以被网络产品和服务的提供者收集和使用。

## 2. 通过合作共享或购买形式从第三方获取用户信息

网络产品和服务提供者若是通过合作共享方式或购买形式从第三方获取并使用用户信息的，首先，应注意审核前述第三方对于用户信息收集的来源是否合法，若其来源不合法，则不得对该等用户信息进行收集和使用。其次，应注意审核前述第三方将用户信息共享或出售给网络产品和服务提供者进行使用的行为是否已取得用户信息所有者的完整、合法、有效的授权。换言之，网络产品和服务提供者通过第三方获取并使用用户信息时，除应取得前述第三方的合法有效的授权外，仍须注意遵从现行法律法规的要求，向用户信息的所有人明示网络产品和服务提供和对于用户信息的收集/使用的目的、方式和范围并取得用户信息所有者的同意。实践中，鉴于网络产品和服务提供者有时可能并不会与用户信息所有者直接接触并达成用户信息保护的有关约定，因此，网络产品和服务提供者往往会要求前述第三方协助（如通过前述第三方的用户服务协议等方式）其向用户信息所有者披露网络产品和服务提供者的存在及网络产品和服务收集、使用用户信息的目的、方式和范围，以此方式来取得用户信息所有者的充分授权。否则，若无用户信息所有者的同意，网络产品和服务的提供者不得对该等用户信息进行收集和使用，除非该等用户信息已经前述第三方进行脱敏/去识别化处理且不能复原。再次，网络产品和服务的提供者应与前述第三方签订合作协议/购买协议，明确约定用户信息的数据权属，用户信息的授权使用期限、方式、范围及用途，协议各方有关用户信息保护的责任等内容。最后，网络产品和服务提供者在从前述第三方获取用户信息时，也应注意遵从有关法律、行政法规及数据共享/交易的有关国家标准及行业标准等的要求。

## 3. 通过网络收集用户信息

目前，网络产品和服务通过网络收集用户信息的方式包括但不限于公开 API 或爬虫等。而其中被更为广泛应用且较为容易引起法律遵从争议的用户信息收集方式则为通过爬虫方式获取用户信息。当网络产品和服务提供者通过爬虫方式在网络上获取第三方的用户信息数据时，应注意遵从作为数据来源的第三方所设置

的“网络爬虫排除标准”（Robots Exclusion Protocol, Robots 协议），通过 Robots 协议来判断哪些数据可以抓取，哪些数据不得抓取。同时，网络产品和服务提供者应注意，鉴于通过爬虫方式获取的用户信息数据时，往往无法明确取得用户信息所有者的同意，因此在收集数据过程中，应避免收集尚未被用户信息所有者公开发布的相关信息数据（如用户个人隐私数据、商业秘密等），以免构成对用户信息所有者合法权益的侵犯。

《网络安全法》第四十条的规定：网络运营者应当对其收集的用户信息严格保密，并建立健全用户信息保护制度。因此，无论用户信息的收集采用的是何种方式，网络产品和服务提供者均对其收集的用户信息负有保密义务。

此外，不论网络产品和服务提供者利用何种技术手段或方式通过收集用户信息，均不得违反国家规定，侵入第三方计算机信息系统或者采用其他技术手段，获取该计算机信息系统中存储、处理或者传输的数据，否则，情节严重的，将构成刑事犯罪，依法受到刑事处罚。且未经用户信息所有者的合法有效授权，网络产品和服务提供者不应以任何手段获取含有商业秘密乃至国家秘密的用户信息，以免触发刑事犯罪风险。

## （二）用户信息的传输存储

### 1. 用户信息传输存储的安全保障

网络产品和服务提供者在对用户信息的传输存储过程中，应对用户信息采取分类分级管理，将含有个人信息、个人隐私、商业秘密乃至国家秘密等敏感信息数据的用户信息（以下简称“敏感用户信息”）与其他用户信息进行区分管理。对于敏感用户信息的传输存储应采取比其他用户信息更为严格的安全保护措施，且对于前述含有敏感用户信息的传输存储应符合我国现行法律、行政法规和国家与行业相关标准的要求，并应采取更为严格的加密措施，以此保障敏感用户信息在传输存储中的机密性、完整性和真实性。同时，对于敏感用户信息和其他用户信息的传输存储和内部访问权限予以明确区分，对敏感用户信息配置更为严格的访问控制规则和操作规程，明确敏感用户信息传输存储的控制策略及敏感用户信息存储安全的负责人。并且，为有效保障用户信息的安全，网络产品和服务提供者应时刻关注加密技术及其他信息安全保护技术的更新并尽最大努力将其运用于网络产品

和服务中，保障存储用户信息的信息系统的安全，防止用户信息在存储过程中发生泄露。

## 2. 用户信息的存储期限

网络产品和服务对于用户信息的存储期限应根据其业务具体运营的内容及形式严格遵从我国现行法律法规的有关规定，主要包括但不限于表 20-2 中的规定。

表 20-2 存储期限规定

法规名称	用户信息保存要求及期限
《互联网信息服务管理办法（2011 修订）》	第十四条规定，从事新闻、出版以及电子公告等服务项目的互联网信息服务提供者，应当记录提供的信息内容及其发布时间、互联网地址或者域名；互联网接入服务提供者应当记录上网用户的上网时间、用户账号、互联网地址或者域名、主叫电话号码等信息。互联网信息服务提供者和互联网接入服务提供者的记录备份应当保存 60 日，并在国家有关机关依法查询时，予以提供
《移动互联网应用程序信息服务管理规定》	第七条规定，移动互联网应用程序提供者应当严格落实信息安全管理责任，记录用户日志信息，并保存 60 日
《移动智能终端应用软件预置和分发管理暂行规定》	第五条规定，为移动智能终端应用软件提供代收费的企业，应对用户确认信息和计费原始数据至少保存 5 个月，并为用户查询提供方便
《网络交易管理办法》	第三十条规定，第三方交易平台经营者对平台内经营者（第三方店铺的经营者）的营业执照或者个人真实身份信息记录保存时间从经营者在平台的登记注销之日起不少于两年，交易记录等其他信息记录备份保存时间从交易完成之日起不少于两年
《网络游戏管理暂行办法》	第十九条规定，网络游戏运营企业发行网络游戏虚拟货币的，应当保存网络游戏用户的购买记录。保存期限自用户最后一次接受服务之日起，不得少于 180 日。 第二十条规定，网络游戏虚拟货币交易服务企业应当保存用户间的交易记录和账务记录等信息不得少于 180 日
《互联网直播服务管理规定》	第十六条规定，互联网直播服务提供者应当记录互联网直播服务使用者发布内容和日志信息，保存 60 日
《网络预约出租汽车经营服务管理暂行办法》	第十八条及二十七条规定，网约车平台公司应当记录驾驶员、约车人在其服务平台发布的信息内容、用户注册信息、身份认证信息、订单日志、上网日志、网上交易日志、行驶轨迹日志等数据并备份。网约车平台公司应当遵守国家网络和信息安全有关规定，所采集的个人信息和生成的业务数据，应当在中国内地存储和使用，保存期限不少于两年
《网络借贷信息中介机构业务活动管理暂行办法》	第二十三条规定，网络借贷信息中介机构应当采取适当的方法和技术，记录并妥善保存网络借贷业务活动数据和资料，做好数据备份。保存期限应当符合法律法规及网络借贷有关监管规定的要求。借贷合同到期后应当至少保存 5 年

### 3. 用户信息的存储地域

《个人信息和重要数据出境安全评估办法（草案）》<sup>①</sup>规定，网络运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据，应当在境内存储。因业务需要，确需向境外提供的，应当按照本办法进行安全评估。重要数据，是指与国家安全、经济发展，以及社会公共利益密切相关的数据，具体范围参照国家有关标准和重要数据识别指南。《信息安全技术 数据出境安全评估指南（草案）》中进一步将重要数据界定为“我国政府、企业、个人在境内收集、产生的不涉及国家秘密，但与国家安全、经济发展以及公共利益密切广的数据（包括原始数据和衍生数据）”，一旦未经授权披露、丢失、滥用、篡改或销毁，或汇聚、整合、分析后，可能造成损害国家财产、社会公共利益和个人合法权益，危害国家关键基础设施、关键信息基础设施、政府系统信息安全，影响或危害国家政治、国土、军事、经济、文化、社会、科技、信息、生态、资源、核设施等其他国家安全事项等后果。如对用户访问互联网日志数据、用户计费数据和上网记录等个人通信数据来说，在关键领域或重要行业中在使用电子信息产品的过程中采集、存储、管理和分析的涉及政府秘密、商业秘密和个人隐私的信息，电子商务交易记录以及相关的个人消费习惯及偏好和企业经营数据等均属于其行业（领域）内的重要数据。

因此，网络产品和服务提供者应将用户信息进行分类管理，对于含有个人信息及重要数据的用户信息，以及其他法律、行政法规规定应在中国境内存储、处理和分析的用户信息数据，应严格将该等用户信息的存储、处理和分析限制在中国境内进行。否则，网络产品和服务提供者将被有关主管部门（如网信部门、公安机关、通信主管部门等）按其职责依照相关法律法规规定给予处罚。并且，若网络产品和服务提供者给用户信息主体造成损失的，将依法承担民事责任；涉嫌犯罪的，将被依法追究刑事责任。

据公开报道，为更符合《网络安全法》等现行有关法律法规的要求，苹果公司已于2017年7月12日与贵州省政府共同签订《贵州省人民政府苹果公司 iCloud 战略合作框架协议》，约定苹果公司将在贵安新区注册实体公司，与云上贵州大数据产业发展有限公司合作建设 iCloud 贵安新区主数据中心，项目落成后，中国用

---

<sup>①</sup> 由全国信息安全标准化技术委员会于2017年5月27日公布，性质为国家推荐标准。

户数据将存储在中国大陆的数据中心。

### （三）用户信息的使用

我国当前对于用户信息使用的规定主要集中在对于用户个人信息的使用方面，如《网络安全法》、《电信和互联网用户个人信息保护规定》、《网络交易管理办法》等多部现行法律法规均明确规定，网络服务提供者使用个人信息应当遵循合法、正当、必要的原则，并应对个人信息严格保密，不得泄露、篡改、出售或非法向他人提供。同时，《网络安全法》中也明确规定了对于个人信息使用的例外情形，即经过处理无法识别特定个人且不能复原的除外。也有部分法规明确规定了对于不含用户个人信息的其他用户信息的保护义务，如《网络交易管理办法》中明确规定网络商品经营者、有关服务经营者及其工作人员对收集的经营者商业秘密的数据信息必须严格保密，不得泄露、出售或者非法向他人提供。《互联网新闻信息服务管理规定》中除明确规定互联网新闻信息服务提供者对用户身份信息负有保密义务外，还规定互联网新闻信息服务提供者对用户的日志信息负有保密的义务，不得泄露、篡改、毁损，不得出售或非法向他人提供。

有鉴于此，网络产品和服务提供者在使用用户信息的过程中，也应对敏感用户信息和其他用户信息进行区分管理。对于敏感用户信息的使用应严格遵从有关法律、行政法规，国家和行业标准的要求，以及网络产品和服务提供者之间达成的约定，严格按照网络产品和服务提供者与用户约定的目的、方式和范围进行使用，不得泄露、篡改、毁损、或未经用户同意擅自出售或向他人提供，除非该等敏感用户信息已经过数据脱密或匿名化处理且不能复原。对于敏感用户信息之外的其他用户信息的使用，也应遵从有关法律、行政法规的规定，若法律、行政法规未明确规定的，网络产品和服务提供者原则上仍应在用户授权范围内对该等用户信息进行使用。若用户信息是从第三方获取的，网络产品和服务提供者还应注意遵从前述第三方约定的使用限制，并应在合法、合理范围内对用户信息进行使用，以免构成不正当竞争行为。例如，新浪微博诉脉脉不正当竞争一案中，二审法院经审理认定脉脉未经新浪微博用户的同意及新浪微博的授权，获取、使用脉脉用户手机通讯录中非脉脉用户联系人与新浪微博用户对应关系的行为，违反了诚实信用原则及公认的商业道德，损害了互联网行业合理有序公平的市场竞争秩

序，一定程度上损害了新浪微博的竞争优势及商业资源，根据《反不正当竞争法》第二条的规定，脉脉展示前述对应关系的行为构成不正当竞争行为。

此外，网络产品和服务提供者应采取措施强化对接触到用户信息尤其是敏感用户信息的有关人员及合作方的授权管理和审计，严格控制用户信息的访问和使用权限，并对用户信息的使用操作进行记录和管理。

#### （四）用户信息的转移共享

网络产品和服务提供者在与第三方合作共享用户信息时，应尤为对于用户信息安全风险的评估和防控，采取技术措施和其他必要措施保障用户的信息安全。

##### 1. 评估确认可以进行转移共享的用户信息

首先，网络产品和服务提供者应对哪些用户信息内容能够进行转移共享进行评估确认，并保障进行转移共享的用户信息中不含有法定禁止转移的信息内容。如《未成年人保护法（2012 修正）》的规定，任何组织或者个人不得披露未成年人的个人隐私。对未成年人的信件、日记、电子邮件，任何组织或者个人不得隐匿、毁弃；除因追查犯罪的需要，由公安机关或者人民检察院依法进行检查，或者对无行为能力的未成年人的信件、日记、电子邮件由其父母或者其他监护人代为开拆、查阅外，任何组织或者个人不得开拆、查阅。鉴此，网络产品和服务提供者对于如未成年人的电子邮件及其他含有未成年人个人隐私的用户信息，不得进行查阅，也不得向第三方合作方进行转移共享，以免侵犯未成年人隐私。再如，我国《宪法》第四十条规定，中华人民共和国公民的通信自由和通信秘密受法律的保护。除因国家安全或者追查刑事犯罪的需要，由公安机关或者检察机关依照法律规定的程序对通信进行检查外，任何组织或者个人不得以任何理由侵犯公民的通信自由和通信秘密。因此，网络产品和服务提供者应保障用户的通信秘密，不得对用户通信进行检查或向第三方提供用户的通信秘密。

其次，对于不属于法定禁止转移共享的敏感用户信息应进行脱敏/去识别化处理且不能复原，以保障对于该等用户信息的转移共享不会对用户信息所有人的合法权益造成损坏。若前述敏感用户信息因实现网络产品和服务功能的需要不能进行脱敏/去识别化处理的，网络产品和服务提供者在对该等用户信息实施转移共享

前，仍应向用户明确其转移共享用户信息的目的、方式和范围，以及第三方对该等用户信息收集和使用的目的、方式和范围，并取得用户的同意，否则不应转移共享该等用户信息。

## 2. 评估确认用户信息的信息安全保护能力

首先，网络产品和服务提供者在选定接收用户信息的第三方前，可以《信息安全技术 数据出境安全评估指南（草案）》作为参考蓝本，从主体（如应具有合法资质、经营范围应与接收数据类型、内容相一致等）、管理保障能力和技术保障能力等方面审查接收用户信息的第三方对于用户信息安全的保护能力。若经评估后，前述第三方不满足用户信息收集和使用的合法、正当、必要原则或不满足用户信息保护的风险可控要求的，则网络产品和服务提供者不应与其合作，向其共享用户信息。

其次，若确认上述第三方可以作为转移共享的用户信息的接收方时，网络产品和服务提供者还应与其签订书面合作协议，明确约定转移共享的用户信息的权属和授权使用的目的、方式、范围和期限，确定与前述第三方对于用户信息保护有关的责任分配，并应要求作为前述第三方对于用户信息保护的标准和采取的安全保护措施均不应低于网络产品和服务提供者的用户信息保护标准，以保障用户信息转移共享后的风险安全可控。

此外，若需转移共享的用户信息属于我国现行法律、行政法规明确规定应在境内存储、分析、使用的信息数据的，网络产品和服务提供商首先不应将其转移共享至在我国境外运营的第三方；应对接收用户信息的第三方予以明确的授权限制，要求其应遵从相关法律法规的要求仅在中国境内对有关用户信息进行存储、分析和使用。

## （五）用户信息的删除

《关于加强网络信息保护的決定》中规定，公民发现泄露个人身份、散布个人隐私等侵害其合法权益的网络信息，或者受到商业性电子信息侵扰的，有权要求网络服务提供者删除有关信息或者采取其他必要措施予以制止。《网络安全法》中也规定了用户对于个人信息的删除权。

因此，对于敏感用户信息，网络产品和服务提供者应依法保障用户的删除权，在相关用户信息的法定保存期限届满后，应按照用户的请求或双方的书面约定对该等用户信息予以删除。但经过脱敏/去识别化且不能复原的用户信息，由于其无法再识别用户个人身份、个人隐私或其他敏感信息，则可以不受上述限制。

此外，网络产品和服务提供者对于内部相关实施部门/人员在用户信息处理过程中的安全管理责任的设置，则可将管理指南草案在其大数据安全管理方法中所确定的大数据主要活动实施部门的安全管理责任（见表 20-3）作为参考蓝本，参照管理指南草案的有关规定执行。

表 20-3 《管理指南草案》大数据主要活动实施部门的安全管理责任

部门	安全管理责任
数据收集实施部门	定义采集数据目的和用途，明确数据采集源和采集数据范围。 遵循意图合规原则，明确数据收集的合法性、正当性和必要性，且只采集满足业务所需的最小数据集。 遵守质量保障原则，指定数据质量保障的策略、规程和要求。 对数据采集环境、采集设施和采集技术采取必要的安全管控措施。 遵循数据保护原则，对收集数据进行分类分级标识，并对不同类别和级别的数据实施相应的安全管理策略和保障措施
数据存储实施部门	先对存储数据进行分类分级，非涉密数据根据管理指南草案的分级要求进行分级。 遵守数据保护原则，并相互考虑存储架构安全、逻辑存储安全、存储访问控制、数据副本安全、数据归档安全、数据时效性管理等几个方面。 建立数据存储冗余策略和管理制度，以及数据备份与恢复操作过程规范
数据使用实施部门	依据国家个人信息和重要数据保护的法律法规要求建立数据使用正当性原则，明确数据使用和分析处理的目的和范围。 建立数据使用的内部责任制度，保证在数据使用声明的目的和范围内对受保护的数据进行使用和分析处理。 遵守最小授权原则，提供细粒度访问控制机制，限定数据使用过程中可访问的数据范围和使用目的。 遵守数据保护原则，主要考虑分布式处理安全、数据分析安全、数据加密处理、数据脱密处理、数据脱敏处理、数据溯源等几个方面。 遵守可审计原则，记录和管理数据使用操作。 对数据分析结果的风险进行合规性评估，避免分析结果输出中包含可恢复的敏感数据
数据分发实施部门	遵守责任不随数据转移原则，对数据分发后产生的数据安全事件承担必要的责任。 在数据分发前，对数据进行风险评估，确保数据分发后的风险可承受，方可分发数据，并通过合同明确数据接收方的数据保护责任。



续表

数据分发实施部门	<p>在数据分发前，对数据的敏感性进行评估，根据评估结果对需要分发的敏感信息进行脱敏操作。</p> <p>遵守可审计原则，记录时间、分发需求，数据接收方等相关信息。</p> <p>提供有效的数据共享访问控制机制，明确不同机构或部门、不同身份与目的的用户的权限，保证访问控制的有效性。</p> <p>建立大数据公开的审核制度，严格审核发布信息复核相关法律法规要求。明确数据公开内容、权限和使用范围，信息发布者与使用者的权利和义务。定期审查公开发布的信息中是否含有非公开信息，一经发现，立即删除。</p> <p>评估数据传输安全风险，明确数据传输安全要求</p>
数据删除实施部门	<p>立即删除超出收集阶段明确的数据留存期限的相关数据；对留存期限有明确规定的，按相关规定执行。</p> <p>在删除数据可能影响执法机构调查取证时，采取适当的存储和屏蔽措施。</p> <p>依照数据分类分级建立相应的数据销毁机制，明确销毁方式和销毁要求。</p> <p>遵守审计原则，建立数据销毁策略和管理制度，明确销毁数据范围和流程，记录数据删除的操作时间、操作人、操作方式、数据内容等相关信息</p>

三、其他有关用户信息保护的制度规定

（一）配合网络安全审查

《网络产品和服务安全审查办法（试行）》规定，关系国家安全的网络和信息  
系统采购的重要网络产品和服务，应当经过网络安全审查。重点对网络产品和服务  
提供者利用提供产品和服务的便利条件非法收集、存储、处理、使用用户相关  
信息的风险等方面进行审查，保障网络产品和服务的安全性、可控性。因此，当  
网络产品和服务为关系国家安全的网络和信息系统提供服务时，网络产品和服务  
提供者应依法配合网络安全审查工作，并对提供材料的真实性负责。

（二）用户信息泄露的告知义务

为充分保障用户对于用户信息的知情权、选择权和隐私权，网络产品和服务  
提供者应在发生或可能发生用户敏感信息或其他重大数据泄露、毁损、丢失的情  
况时，应当立即采取补救措施，按照有关法律规定及时告知用户，并向有关主管  
部门报告。

（三）用户信息保护义务的除外情形

目前，对于进行脱敏/去识别化处理且无法复原的用户信息，由于其经过处理已无法识别原始的用户信息内容，对于该等信息的使用或公开不会再构成对用户信息所有人合法权益的侵害，因而我国现行法律、行政法规并未规定对该等信息的使用限制及用户信息保护义务。

此外，《最高人民法院关于审理利用信息网络侵害人身权益民事纠纷案件适用法律若干问题的规定》明确规定了六种利用网络公开自然人基因信息、病历资料、健康检查资料、犯罪记录、家庭住址、私人活动等个人隐私和其他个人信息的免责情形，即“（一）经自然人书面同意且在约定范围内公开；（二）为促进社会公共利益且在必要范围内；（三）学校、科研机构等基于公共利益为学术研究或者统计的目的，经自然人书面同意，且公开的方式不足以识别特定自然人；（四）自然人自行在网络上公开的信息或者其他已合法公开的个人信息；（五）以合法渠道获取的个人信息；（六）法律或者行政法规另有规定”。但仍应注意，若网络服务提供者以违反社会公共利益、社会公德的方式公开前述第四项、第五项规定的个人信息，或者公开该信息侵害权利人值得保护的重大利益则网络服务提供者仍应依法承担侵权责任。

第三节 网络产品和服务的用户信息保护  
法规遵从框架及建议

网络产品和服务对于用户信息的保护应根据其业务具体运营的内容及形式严格遵从我国现行法律法规的有关规定，主要包括但不限于表 20-4 中规定。

表 20-4 网络产品和服务的信息收集法规遵从框架

法律名称	法律条款	法律规定
《网络安全法》	第二十二条	网络产品、服务具有收集用户信息功能的，其提供者应当向用户明示并取得同意；涉及用户个人信息的，还应当遵守本法和有关法律、行政法规关于个人信息保护的规定

续表

法律名称	法律条款	法律规定
《移动互联网应用程序信息服务管理规定》	第七条	移动互联网应用程序提供者应当严格落实信息安全管理责任，依法履行以下义务：（二）建立健全用户信息安全保护机制，收集、使用用户个人信息应当遵循合法、正当、必要的原则，明示收集使用信息的目的、方式和范围，并经用户同意
	第七条	移动互联网应用程序提供者应当严格落实信息安全管理责任，依法履行以下义务：（六）记录用户日志信息，并保存 60 日
	第八条	互联网应用商店服务提供者应当对应用程序提供者履行以下管理责任：督促应用程序提供者保护用户信息，完整提供应用程序获取和使用用户信息的说明，并向用户呈现
《移动智能终端应用软件预置和分发管理暂行规定》	第五条	生产企业和互联网信息服务提供者所提供移动智能终端应用软件不得调用与所提供服务无关的终端功能、违法发送商业性电子信息；未经明示且经用户同意，不得实施收集使用用户个人信息、开启应用软件、捆绑推广其他应用软件等侵害用户合法权益或危害网络安全的行为
	第六条	生产企业和互联网信息服务提供者均应通过用户提示、企业网站等方式明示所提供移动智能终端应用软件的信息，包括名称、功能描述、卸载方法、开发者信息、软件安装及运行所需权限列表等，明确告知用户应用软件收集、使用用户个人信息的内容、目的、方式和范围等
	第八条	从事应用商店等移动应用分发平台服务的互联网信息服务提供者，以及在移动智能终端中预置了移动应用分发平台的生产企业对所提供的应用软件负有以下管理责任：应加强网络安全防护以及对相关人员的教育培训，保障自身系统安全和用户个人信息安全
《网络交易管理办法》	第十八条	网络商品经营者、有关服务经营者在经营活动中收集、使用消费者或者经营者信息，应当遵循合法、正当、必要的原则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。 网络商品经营者、有关服务经营者收集、使用消费者或者经营者信息，应当公开其收集、使用规则，不得违反法律、法规的规定和双方的约定收集、使用信息
	第十八条	网络商品经营者、有关服务经营者及其工作人员对收集的消费者个人信息或者经营者商业秘密的数据信息必须严格保密，不得泄露、出售或者非法向他人提供。网络商品经营者、有关服务经营者应当采取技术措施和其他必要措施，确保信息安全，防止信息泄露、丢失。在发生或者可能发生信息泄露、丢失的情况时，应当立即采取补救措施。网络商品经营者、有关服务经营者未经消费者同意或者请求，或者消费者明确表示拒绝的，不得向其发送商业性电子信息

续表

法律名称	法律条款	法律规定
《网络游戏管理暂行办法》	第十九条	网络游戏运营企业发行网络游戏虚拟货币的,应当保存网络游戏用户的购买记录。保存期限自用户最后一次接受服务之日起,不得少于 180 日
	第二十条	网络游戏虚拟货币交易服务企业应当保存用户间的交易记录和账务记录等信息不得少于 180 日
	第二十一条	网络游戏运营企业应当要求网络游戏用户使用有效身份证件进行实名注册,并保存用户注册信息
	第二十八条	网络游戏运营企业应当按照国家规定采取技术和管理措施保证网络信息安全,包括防范计算机病毒入侵和攻击破坏,备份重要数据库,保存用户注册信息、运营信息、维护日志等信息,依法保护国家秘密、商业秘密和用户个人信息
《互联网直播服务管理规定》	第十二条	<p>互联网直播服务提供者应当按照“后台实名、前台自愿”的原则,对互联网直播用户进行基于移动电话号码方式的真实身份信息认证,对互联网直播发布者进行基于身份证件、营业执照、组织机构代码证等的认证登记。互联网直播服务提供者应当对互联网直播发布者的真实身份信息进行审核,向所在地省、自治区、直辖市互联网信息办公室分类备案,并在相关执法部门依法查询时予以提供。</p> <p>互联网直播服务提供者应当保护互联网直播服务使用者身份信息和隐私,不得泄露、篡改、毁损,不得出售或者非法向他人提供</p>
	第十六条	互联网直播服务提供者应当记录互联网直播服务使用者发布内容和日志信息,保存 60 日
《网络预约出租汽车经营服务管理暂行办法》	第十八条	网约车平台公司应当记录驾驶员、约车人在其服务平台发布的信息内容、用户注册信息、身份认证信息、订单日志、上网日志、网上交易日志、行驶轨迹日志等数据并备份
	第二十六条	<p>网约车平台公司应当通过其服务平台以显著方式将驾驶员、约车人和乘客等个人信息的采集和使用的目的、方式和范围进行告知。未经信息主体明示同意,网约车平台公司不得使用前述个人信息用于开展其他业务。</p> <p>网约车平台公司采集驾驶员、约车人和乘客的个人信息,不得超越提供网约车业务所必需的范围。</p> <p>除配合国家机关依法行使监督检查权或者刑事侦查权外,网约车平台公司不得向任何第三方提供驾驶员、约车人和乘客的姓名、联系方式、家庭住址、银行账户或者支付账户、地理位置、出行线路等个人信息,不得泄露地理坐标、地理标志物等涉及国家安全的敏感信息。发生信息泄露后,网约车平台公司应当及时向相关主管部门报告,并采取及时有效的补救措施</p>

续表

法律名称	法律条款	法律规定
《网络预约出租汽车经营服务管理暂行办法》	第二十七条	网约车平台公司应当遵守国家网络和信息安全有关规定，所采集的个人信息和生成的业务数据，应当在中国内地存储和使用，保存期限不少于两年，除法律法规另有规定外，上述信息 and 数据不得外流
《网络借贷信息中介机构业务活动管理暂行办法》	第十八条	网络借贷信息中介机构应当按照国家网络安全相关规定和国家信息安全等级保护制度的要求，开展信息系统定级备案和等级测试，具有完善的防火墙、入侵检测、数据加密，以及灾难恢复等网络安全设施和管理制度，建立信息科技管理、科技风险管理和科技审计有关制度，配置充足的资源，采取完善的管理控制措施和技术手段保障信息系统安全稳健运行，保护出借人与借款人的信息安全。  网络借贷信息中介机构应当记录并留存借贷双方上网日志信息，信息交互内容等数据，留存期限为自借贷合同到期起 5 年；每两年至少开展一次全面的安全评估，接受国家或行业主管部门的信息安全检查和审计
	第二十三条	网络借贷信息中介机构应当采取适当的方法和技术，记录并妥善保存网络借贷业务活动数据和资料，做好数据备份。保存期限应当符合法律法规及网络借贷有关监管规定的要求。借贷合同到期后应当至少保存 5 年
	第二十七条	网络借贷信息中介机构应当加强出借人与借款人信息管理，确保出借人与借款人信息采集、处理及使用的合法性和安全性。  网络借贷信息中介机构及其资金存管机构、其他各类外包服务机构等应当为业务开展过程中收集的出借人与借款人信息保密，未经出借人与借款人同意，不得将出借人与借款人提供的信息用于所提供服务之外的目的
	第二十七条	在中国境内收集的出借人与借款人信息的储存、处理和分析应当在中国境内进行。除法律法规另有规定外，网络借贷信息中介机构不得向境外提供境内出借人和借款人信息

网络产品、服务除应注意遵从有关法律、行政法规对于用户信息保护的有关要求之外，还应注意遵从网络产品、服务在生产运营过程中涉及的有关国家标准和行业标准的要求或以相关指导性标准（见表 20-5）作为用户信息保护的法规遵从工作的参考蓝本。

表 20-5 网络产品、服务与用户信息保护的法规遵从建议

控制项	网络产品、服务与用户信息保护的法规遵从建议	对应条款
1. 用户信息的保护原则		
合法正当必要原则	对于用户信息的收集、使用须严格遵从法律规定，处理用户信息具有特定、明确、合理的目的，不扩大使用范围，不在用户信息主体不知情的情况下改变处理用户信息的目的	《网络安全法》第二十三条第三款网络产品、服务具有收集用户信息功能的，其提供者应当向用户明示并取得同意；涉及用户个人信息的，还应当遵守本法和有关法律、行政法规关于个人信息保护的规定
明示原则	对用户信息主体要尽到告知、说明和警示的义务。明确如实地向用户信息主体告知收集和处理用户信息的目的、用途、范围和类型以及用户个人信息保护措施等信息	
用户同意原则	收集和处理用户信息前要征得用户信息主体的同意	
最少够用原则	只收集实现产品和服务功能所需的最少用户信息，实现用户信息的收集和处理目的后，在最短时间内删除用户信息	
质量保证原则	实施适当措施确保用户信息的准确性、相关性、完整性和时效性，建立控制机制定期检查收集和存储的用户信息数据的质量	
最小授权原则	在保证业务功能完整实现的基础上应赋予用户收集和使用过程中各角色最小的操作权限，所有角色只能使用所授权范围内的用户信息数据，非授权范围内的用户信息数据的使用必须进行授权审批，防止未经用户信息管理者授权的检索、披露及丢失、泄露、损毁和篡改用户信息	
责任明确原则	明确用户信息收集、处理过程中的责任，采取相应的措施落实相关责任，并对用户信息收集、处理过程进行记录以便于追溯。 若网络产品、服务提供者须转移用户信息数据的，需确保通过合同或其他策略等明确界定了接收方接收用户信息的范围、要求及应承担的用户信息保护责任，确保接收方提供同等或更高的用户信息保护水平	
可审计原则	对用户信息的修改、查询、导出、删除等操作予以记录，且该等记录应可追溯可审查	
2. 用户信息的主要处理活动		
用户信息的收集	定义采集用户信息目的和用途，明确用户信息的采集源和采集数据范围； 明确告知收集用户信息的目的、用途、范围和类型，在用户明示同意后，方可收集用户信息； 要采用已告知的手段和方式直接向用户信息主体收集，不采取隐蔽手段或以间接方式收集用户信息。 只收集实现产品和服务功能所需的最少用户信息，收集的用户信息仅用于用户同意的目的和用途。 应当对其收集的用户信息严格保密，并建立了规范的用户信息保护制度。	

续表

控制项	网络产品、服务与用户信息保护的法规遵从建议	对应条款
用户信息的收集	<p>持续收集用户信息时提供相关功能，允许用户信息主体配置、调整、关闭用户信息收集功能。</p> <p>不直接向未成年人收集用户个人信息，确需收集其个人信息的，要征得其法定监护人的明示同意。</p> <p>遵守质量保障原则，指定用户信息质量保障的策略、规程和要求。</p> <p>遵循数据保护原则，对收集的用户信息进行分类分级标识，并对不同类别和级别的用户信息实施相应的安全管理策略和保障措施</p>	
用户信息的传输存储	<p>对存储的用户信息进行分类分级，非涉密的用户信息数据根据《信息安全技术大数据安全管理指南》的分级要求进行分级。</p> <p>遵守数据保护原则，并相互考虑存储架构安全、逻辑存储安全、存储访问控制、用户信息副本安全、用户信息归档安全、用户信息时效性管理等几个方面。</p> <p>建立用户信息存储冗余策略和管理制度，以及用户信息备份与恢复操作过程规范</p>	
用户信息的使用	<p>依据国家个人信息和重要数据保护的法律法规要求建立用户信息使用正当性原则，明确用户信息使用和分析处理的目的和范围，并采用已告知的方法和手段使用用户信息。</p> <p>未经用户明示同意，不得向他人提供用户个人信息，经处理无法识别特定个人且不能复原的除外。</p> <p>遵守最小授权原则，提供细粒度访问控制机制，限定用户信息使用过程中可访问的用户信息范围和使用目的。</p> <p>遵守数据保护原则，主要考虑分布式处理安全、用户信息分析安全、用户信息加密处理、用户信息脱密处理、用户信息脱敏处理、用户信息溯源等几个方面。保证使用过程中信息系统持续稳定运行，用户信息处于完整、可用状态，且保持最新。</p> <p>遵守可审计原则，记录和管理用户信息使用操作。</p> <p>对用户信息数据分析结果的风险进行合规性评估，避免分析结果输出中包含可恢复的敏感数据。</p> <p>详细记录用户个人信息的状态，用户信息主体要求对其个人信息进行查询时，用户信息管理者要如实并免费告知是否拥有其个人信息、拥有其个人信息的内容、个人信息的使用状态等内容，除非告知成本或者请求频率超出合理的范围</p>	
用户信息的转移共享	<p>不违背收集阶段告知的转移目的，或超出告知的转移范围转移用户信息。</p> <p>遵守责任不随数据转移原则，对用户信息转移共享后产生的用户信息安全事件承担必要的责任。</p>	

续表

控制项	网络产品、服务与用户信息保护的法规遵从建议	对应条款
用户信息的转移共享	<p>在转移共享用户信息前，对用户信息进行风险评估，确保用户信息转移共享后的风险可承受，方可进行转移共享，并通过合同明确数据接收方的用户信息保护责任。</p> <p>在转移共享用户信息前，对用户信息数据的敏感性进行评估，根据评估结果对需要转移共享的敏感信息进行脱敏操作。</p> <p>遵守可审计原则，记录时间、转移共享需求，用户信息接收方等相关信息。</p> <p>提供有效的用户信息共享访问控制机制，明确不同机构或部门、不同身份与目的的用户的权限，保证访问控制的有效性。</p> <p>评估用户信息传输安全风险，明确用户信息传输安全要求。保证转移共享过程中，用户信息不被用户信息接收方之外的任何个人、组织和机构所获知。</p> <p>未经个人信息主体的明示同意，或法律法规明确规定，或未经主管部门同意，个人信息管理者不得将个人信息转移给境外个人信息获得者，包括位于境外的个人或境外注册的组织和机构</p>	
用户信息的国内更正与删除	<p>向用户信息主体提供查询、更正个人信息的功能。</p> <p>收集阶段告知的个人信息使用目的达到后，立即删除个人信息；如需继续处理，要消除其中能够识别具体个人的内容；如需继续处理个人敏感信息，要获得个人信息主体的明示同意。</p> <p>立即删除超出收集阶段明确的留存期限的相关用户信息；对留存期限有明确规定的，按相关规定执行。</p> <p>用户信息主体有正当理由要求删除其个人信息时，及时删除个人信息。删除个人信息可能影响执法机构调查取证时，采取适当的存储和屏蔽措施。</p> <p>依照用户信息分类分级建立相应的信息销毁机制，明确销毁方式和销毁要求。</p> <p>遵守审计原则，建立用户信息销毁策略和管理制度，明确销毁用户信息的范围和流程，记录用户信息删除的操作时间、操作人、操作方式、信息内容等相关信息</p>	
用户信息的泄露	制定个人信息泄露应急预案，当发生个人信息泄露事件时，采取有效措施降低用户的损失	
3. 用户信息的安全保护措施		
分级分类保护	<p>涉密信息的处理、保存、传输、利用按国家保密法规执行。</p> <p>根据搜集、存储和使用的用户信息范围，结合自身行业特点制定用户信息分级分类规范，包括但不限于用户信息分类方法及指南；用户信息分级详细清单，包括不同类别的用户信息的初始安全级别；用户信息分级保护的安全要求。对不同安全级别的数据实施恰当的安全保护措施</p>	
选择适当的保护措施	采取安全措施（如加密存储、安全审计）保护个人信息等重要用户信息的安全，防止泄露、篡改、损毁、丢失	



## 第四节 监督管理与法律责任

### 一、监督管理

对于用户信息保护的监督管理工作，主要由网信部门、公安机关和通信主管部门等按各自职责依照相关法律法规规定实施。若网络产品、服务提供者违反用户信息保护的合规要求的，网信部门、公安机关和通信主管部门等将按照各自职责依法给予处罚。

### 二、法律责任

《网络安全法》第六十四条第一款规定，网络运营者、网络产品或者服务的提供者违反本法第二十二条第三款、第四十一条至第四十三条规定，侵害个人信息依法得到保护的权利的，由有关主管部门责令改正，可以根据情节单处或者并处警告、没收违法所得、处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款；情节严重的，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照。

此外，网络产品、服务提供者给用户信息主体造成损失的，依法将承担民事责任；涉嫌犯罪的，依法将被追究刑事责任。

## 第 21 章

# 保密义务

关键信息基础设施的运营者在建设、运营、维护关键信息基础设施的过程中，必然要向网络产品和服务提供者采购相关产品和服务，为了避免或减轻来源于产品和服务供应链的安全风险，保障关键信息基础设施的安全持续运行，在实践中要求关键信息基础设施的运营者采购网络产品和服务，应当按照规定与提供者签订安全保密协议，明确安全和保密义务与责任。

为了确保关键信息基础设施采购的保密性与安全性，《网络安全法》第三十六条规定，关键信息基础设施的运营者采购网络产品和服务时，应当按照规定与提供者签订安全保密协议，并明确安全和保密义务与责任。

### 第一节 《网络安全法》相关规定及释义

《网络安全法（草案）》第二十九条规定：关键信息基础设施的运营者采购网络产品和服务，应当与提供者签订安全保密协议，明确安全和保密义务与责任。《网络安全法（草案二次审议稿）》第三十四条规定：关键信息基础设施的运营者采购网络产品和服务，应当与提供者签订安全保密协议，明确安全和保密义务与责任。《网络安全法（草案三次审议稿）》第三十六条规定：关键信息

基础设施的运营者采购网络产品和服务，应当按照规定与提供者签订安全保密协议，明确安全和保密义务与责任。《网络安全法》第三十六条规定：关键信息基础设施的运营者采购网络产品和服务，应当按照规定与提供者签订安全保密协议，明确安全和保密义务与责任。从草案、草案二次审议稿到草案三次审议稿以及最终通过的网络安全法的具体规定来看，有关签订安全保密协议的具体规定在变化时增加了“按照规定”，之所以增加“按照规定”，原因在于安全保密协议是一种特殊的合同，基于保障关键信息基础设施安全的需要，安全保密协议的具体条款应有统一的标准。

依照相关法条规定，关键基础设施运营者在采购网络产品和服务时，应依法签订保密协议，其中需要明确安全和保密义务的具体内容，从《网络安全法》维护国家安全、公民财产安全和网络安全产品运营环境安全的利益来看，国家秘密、公民个人隐私和商业秘密是安全保密协议中必要的也是最重要的内容，网络产品和服务的提供者应当根据关键信息基础设施运营者的需求，对自身通过产品和服务提供获取的相关信息予以保密。

## 第二节 保密义务制度概述

### 一、保密义务

保密义务，即网络产品和服务的提供者应当根据关键信息基础设施运营者的需求，对自身通过产品和服务提供获取的相关信息予以保密，这些信息包括国家秘密、商业秘密以及在提供产品或者服务的过程中获取的敏感个人信息。保密协议的作用在于弥补网络安全审查的不足，鉴于审查能力的问题以及网络安全风险的变化性，网络安全审查无法保障百分之百的安全，因此需要其他制度予以弥补。安全协议通过网络产品和服务提供者的承诺以及损害赔偿的威慑，一方面提升其注意义务；另一方面促使其强化对其员工的管理，避免出现道德风险。

## 二、保密的对象和范围

### （一）国家秘密

关系国家的安全和利益；依照法律规定的一定程序加以确定，而不应由任何个人或组织任意确定；在某个确定的时间内只能限于一定范围的人员知道的事项。依照《中华人民共和国保守国家秘密法》的规定。国家秘密的密级分为“绝密”、“机密”、“秘密”。“绝密”是最重要的国家秘密，泄露会使国家的安全和利益遭到特别严重的损害。“机密”是重要的国家秘密，泄露会使国家的安全和利益遭到严重损害。“秘密”是一般的国家秘密，泄露会使国家的安全和利益遭到损害。国家秘密事项的密级一经确定，就要在秘密载体上做出明显的标志。

### （二）个人隐私

个人隐私，是指公民个人生活中不愿为他人公开或知悉的秘密。隐私权是自然人享有的对其个人的、与公共利益无关的个人信息、私人活动和私有领域进行支配的一种人格权。

### （三）商业秘密

按照我国《反不正当竞争法》的规定，商业秘密是指不为公众所知悉、能为权利人带来经济利益，具有实用性并经权利人采取保密措施的技术信息和经营信息。因此商业秘密包括两部分：技术信息和经营信息。例如，管理方法，产销策略，客户名单、货源情报等经营信息；生产配方、工艺流程、技术诀窍、设计图纸等技术信息。商业秘密是企业的财产权利，它关乎企业的竞争力，对企业的发展至关重要，有的甚至直接影响企业的生存。

## 三、安全保密协议的内容与形式

### （一）安全保密协议的内容

（1）对网络产品和服务提供的情况进行保密；

- (2) 对网络产品和服务的技术细节进行保密;
- (3) 对获取的关键信息基础设施运营者的重要和敏感信息予以保密。

同时,关键信息基础设施的运营者可以根据自身需要确定需要保密的信息范围。针对网络产品和服务提供者违反安全保密协议的责任可以参照合同法有关规定,要求其赔偿损失,其违反安全保密协议或拒不履行安全保密义务而构成危害国家安全等刑事犯罪的,还应追究其刑事责任。

## (二) 安全保密协议的形式

关键信息基础设施运营者与网络产品和服务提供者签订的采购相关产品和服务合同,除遵守《网络安全法》的规定外,也应遵守合同法的相关规定。《合同法》第四十三条规定:当事人在订立合同过程中知悉的商业秘密,无论合同是否成立,不得泄露或者不正当地使用。泄露或者不正当地使用该商业秘密给对方造成损失的,应当承担损害赔偿责任。《合同法》第六十条规定:当事人应当按照约定全面履行自己的义务。当事人应当遵循诚实信用原则,根据合同的性质、目的和交易习惯履行通知、协助、保密等义务。因此,网络产品和服务提供者保守在订立和履行合同中知悉的秘密,是合同的应有之意。

安全保密协议包括两种形式:一是作为采购合同的安全保密条款,二是作为单独的安全保密协议。此外,有关安全保密协议的内容由关键信息基础设施的运营者以及网络产品和服务的提供者共同确定,具体包括两个方面,一方面为安全义务,另一方面是保密义务。

## 四、国外保密法律制度

从国外保密立法的调整范围来看,只有少数国家有专门的保密法,我国、俄罗斯和乌克兰等是其中的典型代表。我国于 1988 年颁布了《保密法》,俄罗斯于 1993 年 7 月 21 日颁布实施了《俄罗斯联邦国家保密法》,乌克兰于 1999 年 9 月 21 日经修订后颁布了新的《乌克兰国家秘密法》,除此之外,其他国家并没有一部保守国家秘密的专门法律。西方资本主义法治国家的典型代表如美国、英国、

德国等并没有一部综合性的保守国家秘密法，保密法律制度体现在一些具体的专项的保密法律法规之中，如涉密人员管理的法律制度、规范定密的法律制度等。但这并不妨碍这些国家有独具特色的保密法律制度，如美国和德国的涉密人员保密审查（安全审查）制度、美国的定密复议制度、美国和俄罗斯的保密诉讼制度等。直到最近，美国减少并保护政府秘密委员会才向国会提交了一份统一保密法的立法草案《1998 政府保密改革法》，建议为保密工作制定一部联邦层次的全面而统一的法律，该草案正在国会审议之中。

从法律体系的整体情况来看，各国保密法律法规的基本法源即表现形式是《行政法》和《刑法》，前者调整和规范国家秘密的确定和国家秘密的管理，后者解决泄密承担刑事法律责任的问题。例如，美国的总统行政命令及其他法律法规都是以行政法规的形式调整定密和保密管理的，德国的密件管理规定同样如此，而关于泄密刑事责任的问题则被纳入本国的刑法典之中。考虑到追究泄密刑事法律责任的法律规范，其功能侧重于事后惩治，它是各国刑事法律的必然内容，从保密防范工作的角度研究泄密刑事法律制度不是保密法的主要内容。保密工作是一种对国家秘密采取防范性保护措施的工作，因此，调整和规范定密和保密管理的法律规范在整个保密法律框架中居于主导地位，也是我们研究的重点。基于这种考虑，我们分析和研究国外保密法律制度的重点也就集中在主要表现为行政法的调整定密和保密管理的法律制度上，从中吸取其关于定密和保密管理的有益的法律治理经验。

### 第三节 保密义务法规遵从框架及建议

#### 一、保密义务的法规遵从框架

除了《网络安全法》和《劳动合同法》、《反不正当竞争法》之外，我国还有其他部门法和地方规章制度对关键信息基础设施的运营者采购网络产品和服务时的保密义务与责任有所规定（见表 21-1）。

表 21-1 保密义务的法规遵从框架

法律名称	法律条款	法律规定
《网络安全法》	第三十六条	关键信息基础设施的运营者采购网络产品和服务，应当按照规定与提供者签订安全保密协议，明确安全和保密义务与责任
	第四十条	网络运营者应当对其收集的用户信息严格保密，并建立健全用户信息保护制度
	第四十五条	依法负有网络安全监督管理职责的部门及其工作人员，必须对在履行职责中知悉的个人信息、隐私和商业秘密严格保密，不得泄露、出售或者非法向他人提供
《中华人民共和国政府采购法》	第十一条	政府采购的信息应当在政府采购监督管理部门指定的媒体上及时向社会公开发布，但涉及商业秘密的除外
	第五十一条	供应商对政府采购活动事项有疑问的，可以向采购人提出询问，采购人应当及时做出答复，但答复的内容不得涉及商业秘密
	第五十三条	采购人应当在收到供应商的书面质疑后 7 个工作日内做出答复，并以书面形式通知质疑供应商和其他有关供应商，但答复的内容不得涉及商业秘密
	第八十五条	对因严重自然灾害和其他不可抗力事件所实施的紧急采购和涉及国家安全和秘密的采购，不适用本法
《中华人民共和国政府采购法实施条例》	第四十条	政府采购评审专家应当遵守评审工作纪律，不得泄露评审文件、评审情况和评审中获悉的商业秘密
	第五十条	采购人应当自政府采购合同签订之日起两个工作日内，将政府采购合同在省级以上人民政府财政部门指定的媒体上公告，但政府采购合同中涉及国家秘密、商业秘密的内容除外
《反不正当竞争法》	第十条	经营者不得采用下列手段侵犯商业秘密：（一）以盗窃、利诱、胁迫或者其他不正当手段获取权利人的商业秘密；（二）披露、使用或者允许他人使用以前项手段获取的权利人的商业秘密；（三）违反约定或者违反权利人有关保守商业秘密的要求，披露、使用或者允许他人使用其所掌握的商业秘密。第三人明知或者应知前款所列违法行为，获取、使用或者披露他人的商业秘密，视为侵犯商业秘密。本条所称的商业秘密，是指不为公众所知悉、能为权利人带来经济利益、具有实用性并经权利人采取保密措施的技术信息和经营信息
《合同法》	第四十三条	当事人在订立合同过程中知悉的商业秘密，无论合同是否成立，不得泄露或者不正当地使用。泄露或者不正当地使用该商业秘密给对方造成损失的，应当承担损害赔偿责任
	第六十条	当事人应当按照约定全面履行自己的义务。当事人应当遵循诚实信用原则，根据合同的性质、目的和交易习惯履行通知、协助、保密等义务

续表

法律名称	法律条款	法律规定
《劳动合同法》	第二十三条	用人单位与劳动者可以在劳动合同中约定保守用人单位的商业秘密和与知识产权相关的保密事项。对负有保密义务的劳动者，用人单位可以在劳动合同或者保密协议中与劳动者约定竞业限制条款，并约定在解除或者终止劳动合同后，在竞业限制期限内按月给予劳动者经济补偿。劳动者违反竞业限制约定的，应当按照约定向用人单位支付违约金
	第二十四条	竞业限制的人员限于用人单位的高级管理人员、高级技术人员和其他负有保密义务的人员。竞业限制的范围、地域、期限由用人单位与劳动者约定，竞业限制的约定不得违反法律、法规的规定。在解除或者终止劳动合同后，前款规定的人员到与本单位生产或者经营同类产品、从事同类业务的有竞争关系的其他用人单位，或者自己开业生产或者经营同类产品、从事同类业务的竞业限制期限，不得超过两年
《工业控制系统信息安全防护指南》	十、供应链管理	（一）在选择工业控制系统规划、设计、建设、运维或评估等服务商时，优先考虑具备工控安全防护经验的企事业单位，以合同等方式明确服务商应承担的信息安全责任和义务。（二）以保密协议的方式要求服务商做好保密工作，防范敏感信息外泄
《证券期货业信息安全保障管理办法》	第三十条	核心机构和经营机构应当加强信息安全保密管理，保障投资者信息安全
	第三十七条	核心机构和经营机构在采购软硬件产品或者技术服务时，应当与供应商签订合同和保密协议，并在合同和保密协议中明确约定信息安全和保密的权利和义务

二、保密义务的法规遵从建议

根据我国《网络安全法》第三十六条规定，关键信息基础设施的运营者采购网络产品和服务时，应当按照规定与提供者签订安全保密协议，并明确安全和保密义务与责任。表 21-2 中对关键信息基础设施的运营者采购网络产品和服务时的保密义务责任进行了详细的说明和规定。

表 21-2 保密义务的法规遵从建议

控制项	保密义务的遵从要求	对应条款
签订保密协议	关键信息基础设施的运营者采购网络产品和服务，应当按照规定与提供者签订安全保密协议，明确安全和保密义务与责任	《网络安全法》第三十六条、第四十条、第四十五条



续表

控制项	保密义务的遵从要求	对应条款
商业秘密保密义务	政府采购评审专家应当遵守评审工作纪律，不得泄露评审文件、评审情况和评审中获悉的商业秘密	
个人隐私安全保密义务	依法负有网络安全监督管理职责的部门及其工作人员，必须对在履行职责中知悉的个人信息、隐私和商业秘密严格保密，不得泄露、出售或者非法向他人提供	

第四节 监督管理与法律责任

《网络安全法》第八条明确规定，国家网信部门负责统筹协调网络安全工作和相关监督管理工作。国务院电信主管部门、公安部门和其他有关机关依照本法和有关法律、行政法规的规定，在各自职责范围内负责网络安全保护和监督管理工作。县级以上地方人民政府有关部门的网络安全保护和监督管理职责，按照国家有关规定确定。

第六十四条规定：网络运营者、网络产品或者服务的提供者违反本法第二十二条第三款、第四十一条至第四十三条规定，侵害个人信息依法得到保护的权利的，由有关主管部门责令改正，可以根据情节单处或者并处警告、没收违法所得、处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款；情节严重的，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照。

# 网络关键设备和网络安全专用 产品合规要求

信息技术在促进社会发展的同时也使得信息安全风险成倍增加，关键信息基础设施面临着前所未有的安全威胁。网络关键设备和网络安全专用产品是关键信息基础设施正常运转的齿轮，在网络安全和国家安全的保障中起到不可替代的重要作用。如果确保网络关键设备和网络安全专用产品的安全可控性成为产业界和学界关注的话题。在此背景下，本章将对网络关键设备和网络安全专用产品的合规要求做出具体的分析。

## 第一节 《网络安全法》相关规定及释义

我国《网络安全法》第二十三条规定：网络关键设备和网络安全专用产品应当按照相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求后，方可销售或者提供。国家网信部门会同国务院有关部门制定、公布网络关键设备和网络安全专用产品目录，并推动安全认证和安全检测结果互认，避免重复认证、检测。本条实际上规定了网络关键设备和网络安全专用产品销售

许可制度，其中两个层面的问题值得关注：一是关于网络关键设备和网络安全专用产品的安全认证和检测。根据我国《电信条例》的规定，国务院电信主管部门制定了电信设备进网许可制度，对电信中断设备、无线电通信设备、网间互联设备实行入网检测；根据《计算机信息系统安全保护条例》的规定，对于用于保护计算机信息系统安全的专用硬件和软件产品进行检测；根据认证和认可条例，国务院质监部门建立了信息安全产品认证制度，实施信息安全产品认证。二是关于网络关键设备和网络安全专用产品认证和检测的具体要求。在网络安全实践中，为了确保网络安全，国家多个行政部门可在各自的职责范围内开展网络安全设备和产品的安全认证与检测，由于认证和检测的项目有相互交叉的部分，则会导致重复的认证和检测，造成企业不必要的负担。在此背景下，《网络安全法》要求国家网信部门和国务院的有关部门具体开展制定、公布网络关键设备和网络安全专用产品目录，并推动安全认证和安全检测结果互认，避免重复认证、检测。第一批网络关键设备和网络安全专用产品目录已经于 2017 年 6 月制定并发布，其他也将陆续予以完善和公布。

## 第二节 网络关键设备和网络安全专用产品合规制度概述

### 一、网络关键设备和网络安全专用产品的认证检测概念

按照相关标准和程序对网络关键设备和网络安全专用产品认证、检测是我国标准化立法确立的重要制度，也是国际上的通行做法。所谓认证，根据中国《认证认可条例》的规定，是指“由认证机构证明产品、服务、管理体系符合相关技术规范、相关技术规范的强制性要求或者标准的合格评定活动”；信息安全测试检测是一个统称的概念。用来概括信息系统风险评估、等级保护测评和涉密系统测评三项信息安全方面的测试检测工作。而通过信息安全认证检测活动的开展，可以及时发现信息安全产品、服务和信息系统的缺陷和漏洞，弥补现有技术的不足，

从而加强信息安全产品的安全性和可控性，保障政府乃至普通用户的网络和信息安全。因此，建立和完善信息安全产品认证认可体系已经成为世界各国促进信息安全产业的发展、保障国家安全和经济利益的重要途径。

## 二、网络关键设备和网络安全专用产品合规的作用

我国《网络安全法》第二十三条明确规定了网络关键设备与网络安全专用产品提供者的义务。在安全实践中，对网络关键设备与网络安全专用产品管理方式有三种：一是公安部的计算机信息系统安全专用产品销售许可证，二是工信部的电信产品进网许可证；三是国家认监委的国家信息安全产品认证。在此基础上，《网络安全法》第二十三条还明确了一个关键信息，国家网信部门及相关部门会制定网络关键设备和网络安全专用产品的目录，并且这些产品在不同部门的认证和安全检测结果互认。后续会推出网络相关产品检测的国家标准及认证规范，这对众多网络及安全厂商是个好消息，除了在特殊领域的应用之外，厂商在众多检测机构办理的证书应该能够互通。这样一方面，各厂商有可能少办理一些产品资质；另一方面，可在一定程度上缓解目前各厂商的“资质大战”。

### 第三节 网络关键设备和网络安全专用产品合规法规 遵从框架及建议

#### 一、网络关键设备和网络安全专用产品合规法规遵从框架

按照相关标准和程序对产品进行检测认证，是我国标准化法所确立的重要制度，也是国际层面的通用做法和趋势。我国在网络关键设备和网络安全专用产品法规遵从的主要立法包括国务院电信主管部门依据《电信条例》的规定建立的电信设备进网许可证制度，以及依据《计算机信息系统安全保护条例》所建立的信息安全专用产品销售许可证制度，以及国务院质检部门建立的信息安全产品认证

制度。以上具体的遵从框架如表 22-1 所示。

表 22-1 信息安全产品认证制度

法律法规名称	法律条款	具体规定
《网络安全法》	第二十三条	网络关键设备和网络安全专用产品应当按照相关国家标准的强制性要求,由具备资格的机构安全认证合格或者安全检测符合要求后,方可销售或者提供。国家网信部门会同国务院有关部门制定、公布网络关键设备和网络安全专用产品目录,并推动安全认证和安全检测结果互认,避免重复认证、检测
《电信设备进网管理办法》	第六条	生产企业申请电信设备进网许可,应当附送国务院产品质量监督部门认可的电信设备检测机构出具的检测报告或者认证机构出具的产品认证证书。 检测机构对申请进网许可的电信设备进行检测的依据、检测规程和出具的检测报告应当符合国家或工业和信息化部的规定
《计算机信息系统安全专用产品检测和销售许可证管理办法》	第十条	安全专用产品的生产者应当向经公安部计算机管理监察部门批准的检测机构申请安全功能检测。对在国内生产的安全专用产品,由其生产者负责送交检测;对境外生产在国内销售的安全专用产品,由国外生产者指定的国内具有法人资格的企业或单位负责送交检测。当安全专用产品的安全功能发生改变时,安全专用产品应当进行重新检测
《关于调整信息安全产品强制性认证实施要求的公告》(2009 年第 33 号)	附件	对边界安全、通信安全、身份鉴别与访问控制、数据安全、基础平台、内容安全、评估审计与监控、应用安全 8 类包括防火墙、安全路由器、反垃圾邮件产品在内的 13 种信息安全产品实施强制性认证

二、网络关键设备和网络安全专用产品合规法规遵从建议

网络关键设备和网络安全专用产品合规法规遵从建议如表 22-2 所示。

表 22-2 网络关键设备和网络安全专用产品合规法规遵从建议

网络关键设备和网络安全专用产品合规法规遵从建议	对应条款
1. 网络关键设备和网络安全专用产品的认证、检测	第二十三条 网
网络关键设备和网络安全专用产品的监测认证包括公安部的计算机信息系统安全专用产品销售许可证、工信部的电信产品进网许可证和国家认监委的国家信息安全产品认证。	络关键设备和网 络安全专用产品 应当按照相关国

续表

网络关键设备和网络安全专用产品合规法规遵从建议	对应条款
以上三种模式由于相应法律法规和规章制度的存在，并不会废止，还是同时需要满足。认证或检测中的任何一种方式都符合法律要求。	家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求后，方可销售或者提供。国家网信部门会同国务院有关部门制定、公布网络关键设备和网络安全专用产品目录，并推动安全认证和安全检测结果互认，避免重复认证、检测
公安部的销售许可证和工信部的入网证是基于检测，而国家信息安全产品认证基于认证	
2. 网络关键设备和网络安全专用产品目录	
为加强网络关键设备和网络安全专用产品安全管理，依据《网络安全法》，国家互联网信息办公室会同工业和信息化部、公安部、国家认证认可监督管理委员会等部门制定了《网络关键设备和网络安全专用产品目录（第一批）》。	
列入《网络关键设备和网络安全专用产品目录第一批》的设备和产品，应当按照相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求后，方可销售或者提供。	
网络关键设备和网络安全专用产品认证或者检测委托人，选择具备资格的机构进行安全认证或者安全检测。	
网络关键设备、网络安全专用产品选择安全检测方式的，经安全检测符合要求后，由检测机构将网络关键设备、网络安全专用产品检测结果（含本公告发布之前已经本机构安全检测符合要求、且在有效期内的设备与产品）依照相关规定分别报工业和信息化部、公安部	

第四节 监督管理与法律责任

《网络安全法》第八条规定：国家网信部门负责统筹协调网络安全工作和相关监督管理工作。国务院电信主管部门、公安部门和其他有关机关依照本法和有关法律、行政法规的规定，在各自职责范围内负责网络安全保护和监督管理工作。根据第八条，《网络安全法》规定了网络关键设备及专用产品的监督管理制度，即“1+X”模式：国家网信部门负责统筹协调网络安全工作，国务院电信主管部门、公安部门和其他有关机关依照本法和有关法律、行政法规的规定，在各自职责范围内负责网络安全保护和监督管理工作。但是，我国《网络安全法》并未对于义务主体违反网络关键设备及专用产品遵从义务的不利后果做出明确的规定。但《电信设备进网管理办法》第二十八条规定，违反本办法规定，销售未获得进网许可的电信终端设备的，由省、自治区、直辖市通信管理局责令改正，并处一万元以

上十万元以下罚款。第二十九条规定，违反本办法规定，伪造、冒用、转让进网许可证，编造进网许可证编号或粘贴伪造的进网许可标志的，由工业和信息化部或者省、自治区、直辖市通信管理局没收违法所得，并处违法所得三倍以上五倍以下罚款；没有违法所得或者违法所得不足一万元的，处一万元以上十万元以下罚款。《计算机信息系统安全专用产品检测和销售许可证管理办法》（公安部令第 32 号）第二十条规定，生产企业违反本办法的规定，有下列情形之一的，视为未经许可出售安全专用产品，由公安机关根据《计算机信息系统安全保护条例》的规定予以处罚：①没有申领销售许可证而将生产的安全专用产品进入市场销售的；②安全专用产品的功能发生改变，而没有重新申领销售许可证进行销售的；③销售许可证有效期满，未办理延期申领手续而继续销售的；④提供虚假的安全专用产品检测报告或者虚假的计算机病毒防治研究的备案证明，骗取销售许可证的；⑤销售的安全专用产品与送检样品安全功能不一致的；⑥未在安全专用产品上标明“销售许可”标记而销售的；⑦伪造、变造销售许可证和“销售许可”标记的。第二十一条规定：“检测机构违反本办法的规定，情节严重的，取消检测资格。”

综上，我国对于违反网络关键设备及专用产品遵从义务的不利后果主要为没收违法所得、罚款、取消从业资格等行政处罚措施。

# 反侵权盗版声明

电子工业出版社依法对本作品享有专有出版权。任何未经权利人书面许可，复制、销售或通过信息网络传播本作品的行为；歪曲、篡改、剽窃本作品的行为，均违反《中华人民共和国著作权法》，其行为人应承担相应的民事责任和行政责任，构成犯罪的，将被依法追究刑事责任。

为了维护市场秩序，保护权利人的合法权益，我社将依法查处和打击侵权盗版的单位和个人。欢迎社会各界人士积极举报侵权盗版行为，本社将奖励举报有功人员，并保证举报人的信息不被泄露。

举报电话：(010) 88254396; (010) 88258888

传 真：(010) 88254397

E-mail: [dbqq@phei.com.cn](mailto:dbqq@phei.com.cn)

通信地址：北京市万寿路 173 信箱

电子工业出版社总编办公室

邮 编：100036